

Mit Stellenmarkt

Anzeige
MEHR ZUM GRÜNEN WEBHOSTING AUF SEITE 19
www.df.eu
Premium Hosting. Premium Service.
domain FACTORY

MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

11 November 2008 € 5,50 H 10554

Tutorial:
Linux mit Active Directory

Security:
Web Exploit Toolkits
Gefahr durch Malware-Baukästen

Maschinelle Übersetzung:

Computer als Dolmetscher

Trends, Theorien, Anwendungen



Administration:
NIS abschaffen mit FreeIPA

Vergleichstest:
Widescreen-Backlight-LED-Monitore

Dokumentendesign:
Barrierefreies PDF

Objektorientierte Assistenten:
Wizard-API für Java

Application Server:
Weblogic in Oracle-Ausführung

Embedded Systems:
Performance-Tuning

Green IT:
Energieeffizientes Rechenzentrum

Heise · Österreich € 6,20 Schweiz CHF 10,70 Benelux € 6,70 Italien € 6,70 · iX Magazin für professionelle Informationstechnik · www.ix.de · November 2008

4 199148 505501 11

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Tiefdruck

Passend zur Jahreszeit der nördlichen Hemisphäre zieht am Horizont der IT-Landschaft schweres Wetter auf: Cloud Computing. Seine Entstehung verdankt es dem Symbol für das Netz der Netze. Hinter dem Zeichen der Wolke verbirgt sich die komplexe Struktur der Wege, die im Einzelfall irrelevant ist, da sie nur zeigen soll, dass zwei oder mehr Systeme miteinander in Verbindung stehen.

Cloud Computing steht jedoch für Handfesteres. Da ballen sich bei Herstellern und Dienstleistern Computerressourcen, die teuer bezahlt nur zu einem geringen Teil ausgelastet sind. Und das ist ein Ärgernis, dem Technik und Marketing mit verschiedenen Mitteln zu Leibe rücken wollen – Cloud Computing ist eins davon. Amazon macht es vor und bietet registrierten Kunden nicht nur Speicherplatz, sondern auch Rechenleistung im Web an. Im Grunde eine Methode, mit der die ersten RZ schon Dampf abgelassen und Rechenzeit vermietet haben, wenn auch ohne Internet.

Im Nebulösen bleibt dabei nur, welche Ressourcen der Kunde bei seinem Anbieter gerade nutzt, was ihm getrost egal sein kann, denn er kauft einen Dienst bei jemandem, der ihm etwas ausrechnet, und das muss stimmen. So lässt Amazon niemanden im Ungewissen und nennt sein Angebot Elastic Compute Cloud (EC2 – nein, kein Quadrat): Da verschwindet nix, aber man bleibt flexibel, schließlich ist das ja noch alles Beta.

Doch offensichtlich reicht das nicht. Fast alle in der IT-Branche müssen die frische Brise gespürt haben und halten nun ihre Fähnchen in den Wind. Alle? Nein, es muss einen geben, und der hält das für (frei übersetzt) ausgemachten Blödsinn (stupidity): Richard Stallman, Gründer der Free Software Foundation. Er sieht die Freiheit bedroht, denn Cloud Computing bedeute, die Kontrolle abzugeben. Das klingt wie ein Widerspruch, denn Open Source heißt ja, andere in die Karten gucken lassen, und Cloud Computing wäre ohne Open Source kaum denkbar. Aber der Dienst ist nicht kostenlos verfügbar und es handelt sich nicht um Verträge mit einer Community. Die Front, die dort aufzieht, droht nicht nur die Dämme der Informationsflut aufzuweichen, sondern auch die Software ins Schwimmen zu bringen.

Eine solche Atmosphäre ruft andere Wolkenmacher auf den Plan: Microsoft in Gestalt von Steve Ballmer, der auf der Bühne immer wieder der Kamera entkommend einen gewaltigen Wirbel verursacht und ein neues Betriebssystem mit dem (vorläufigen) Namen Windows Cloud als unbedingt erforderlich ankündigt. Erst jetzt erkennt man die grenzenlose Freiheit über den Wolken: den Desktop im Internet, was diesmal wohl nicht bei iDOS oder iWin beginnt. Das überraschte Amazon, Google nicht, dort hat man schon – einen Desktop. Amazon ließ deshalb eiligst Windows als Ballon im EC2 steigen. Die Großwetterlage hat nun wohl alle Bereiche erfasst, nicht nur diejenigen, denen es um die gelegentliche Nutzung fremder Ressourcen für spezielle Aufgaben oder um das Abfangen von Leistungsspitzen geht.

Einer, der sich auskennen muss mit wallenden Nebeln und Weissagungen, Larry Ellison, der Chef von Oracle, gab sodann den Derwisch „Gibberish, Insane, and Idiocy“, was man als dummes Gerede, Irrsinn und Idiotie übersetzen kann – und das, nachdem wenige Tage vorher sein Unternehmen groß bei Amazons EC2 eingestiegen war. „Die Computerindustrie ist noch modeverrückter als die Frauen“, räsoniert er weiter und er hat recht, denn Oracle hat sich ja bei Amazon gerade neu eingekleidet. Und er gesteht, dass er gar nicht weiß, worüber alle gerade reden. Auch da hat er recht. Denn was nun Cloud Computing wirklich ist, ein Rechnerverleih, ein dienstbarer Geist oder die endgültige Freiheit vom Desktop, kann keiner mehr sagen. Nur eins ist klar: Es gibt einen neuen Hype.

Ralph Hülsenbusch

RALPH HÜLSENBUSCH



iX-Link ix0811003

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

MARKT + TRENDS

Embedded Systems
Kompakter Industrie-PC unter Linux 14

Internet
eco-Kongress 2008:
Mangelware IPv4-Adressen 16

Systeme
Lenovo geht mit
Servern an den Markt 22

DMS-Expo
Content-Management-Systeme
auf einen Blick 24

Sicherheit
Zutrittskontrolle und
Zeiterfassung per Handy 28

Hardware
AMD mit neuen Profi-Grafikkarten 30

Linux
Mono 2.0 freigegeben 32

Beruf
Wunscharbeitgeber: Google jetzt vor SAP 37

Wirtschaft
Marktforscher sagen
über 5 % IT-Wachstum voraus 38

TITEL

Computer als Dolmetscher
Hauptströmungen
der maschinellen Übersetzung COVER THEMA 42

Übersetzungssoftware:
Integration in Unternehmens-IT 48

REVIEW

Laptops
Netbooks mit Atom-CPU
von Acer und Asus 54

Notebook
Acers Notebook mit
AMDs Turion: Travelmate 5330 58

Datensicherheit
Laptop von Dell
mit geschützter Platte 60

LCDs
Drei Monitore mit RGB-LED-Backlight COVER THEMA 64

Virtualisierung
VMware Fusion 2.0 für Intel-Macs 70

Server-Virtualisierung
Citrix Xenserver 5 74

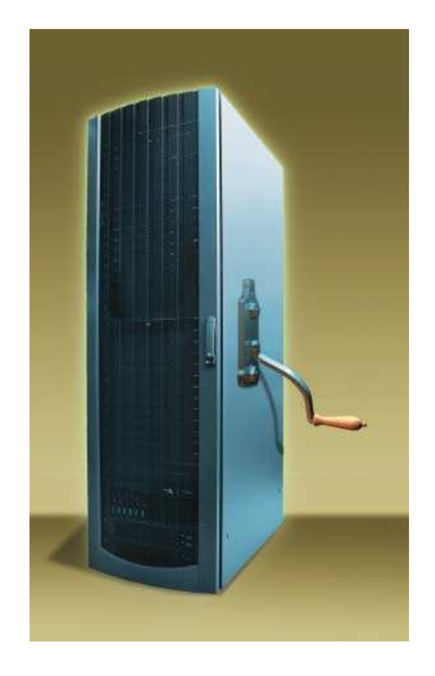
Application Server
Noch Bea-lastig:
Oracle Weblogic Server 10gR3 COVER THEMA 78

Embedded-Hypervisor
Primergy-Server mit
VMwares ESXi embedded 81

REPORT

Publishing
Schwierigkeiten beim
Erstellen barrierefreier PDFs COVER THEMA 84

Recht
Höhere Gewalt in
Verträgen berücksichtigen 92



Strom sparen im RZ

Mehr Energieeffizienz im Rechenzentrum beruhigt nicht nur das Klima-Gewissen, sondern senkt auch die Stromrechnung. Die IT-Hersteller haben bereits reagiert und bieten „grüne“ Komponenten und Konzepte an.

Seite 96

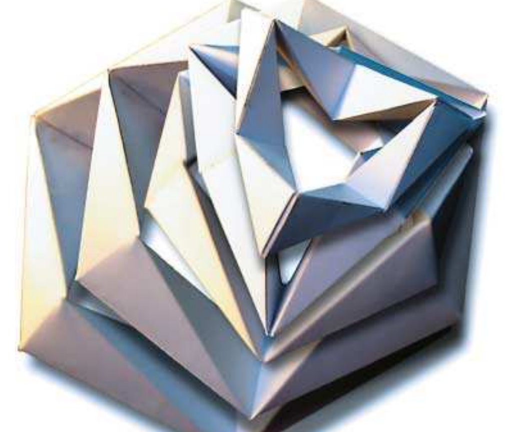
Administration: NIS ade mit FreeIPA

Der einst unter dem Begriff „Yellow Pages“ firmierende Verzeichnisdienst Network Information Service kann aktuelle Sicherheitsanforderungen nicht erfüllen. Kostenlose Abhilfe verspricht das Open-Source-Projekt FreeIPA.

Seite 122



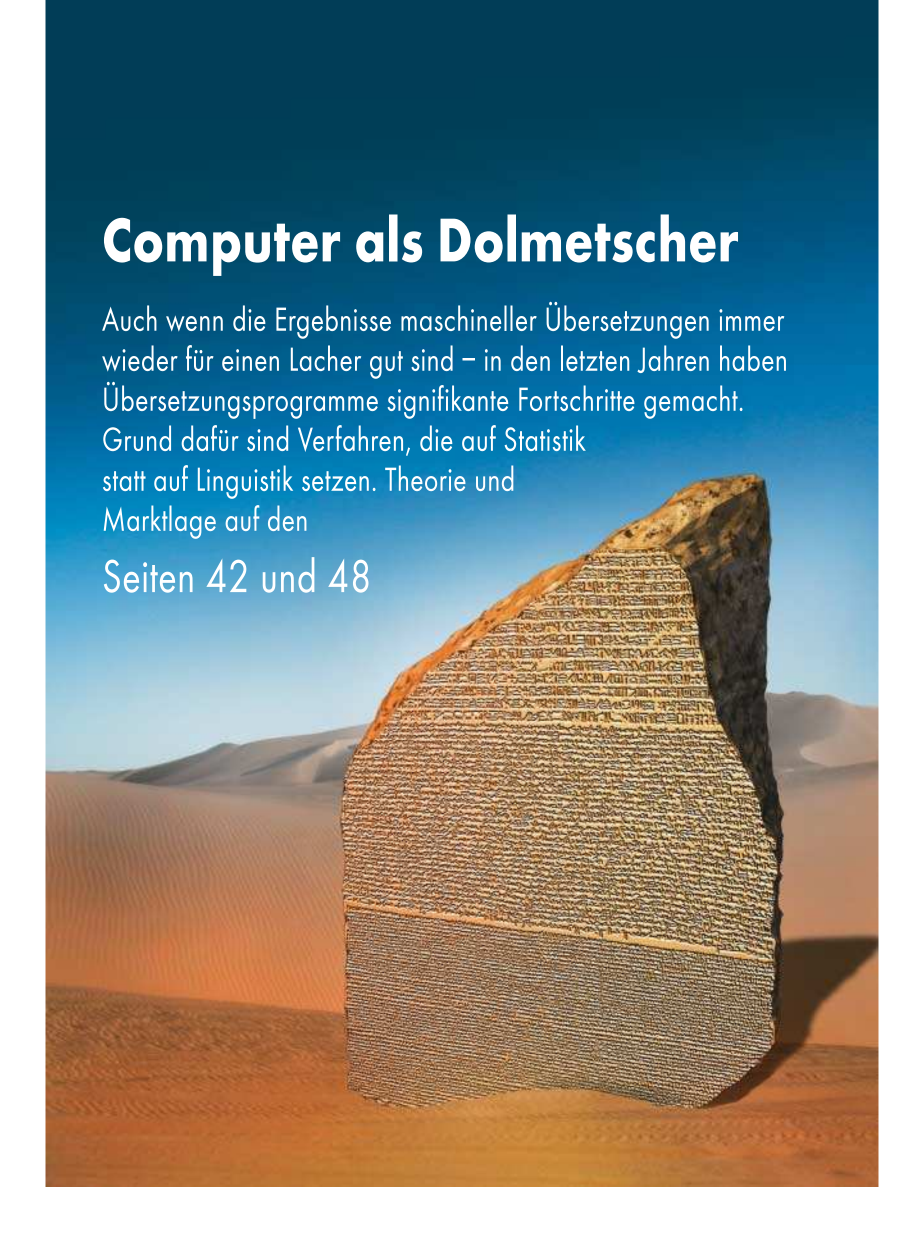
Malware-Baukasten: Web Exploit Toolkit



Wie am Fließband kann man mit Web Exploit Toolkits Malware generieren – was Standard-Anti-Virus-Software große Schwierigkeiten bereitet.

Seite 131

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Computer als Dolmetscher

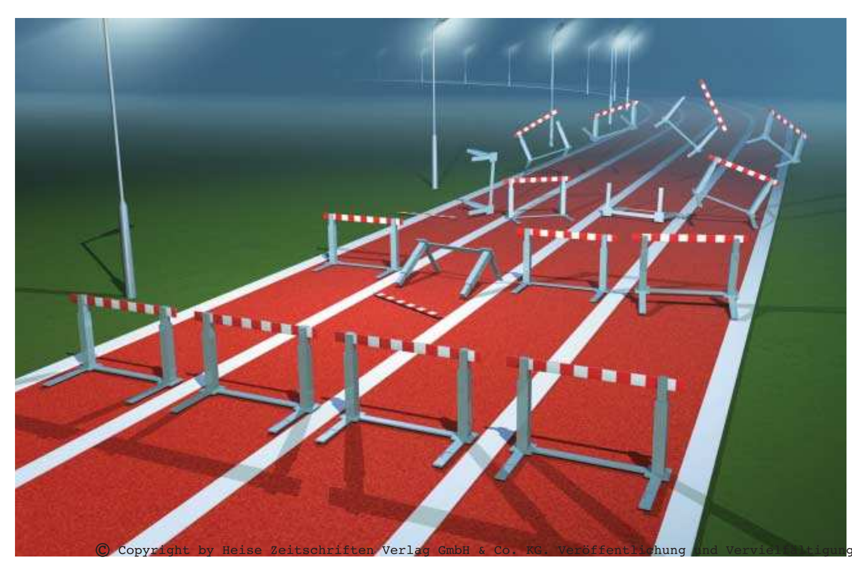
Auch wenn die Ergebnisse maschineller Übersetzungen immer wieder für einen Lacher gut sind – in den letzten Jahren haben Übersetzungsprogramme signifikante Fortschritte gemacht. Grund dafür sind Verfahren, die auf Statistik statt auf Linguistik setzen. Theorie und Marktlage auf den

Seiten 42 und 48

Wege zum barrierefreien PDF

Behörden müssen und Firmen sollten ihre Dokumente barrierefrei erstellen, also deren Inhalt für Menschen mit Behinderungen zugänglich machen. Doch was mit HTML passabel funktioniert, entpuppt sich mit Adobes PDF als steiniger Weg, der nicht immer zum Ziel führt.

Seite 84



Internet
25 Jahre Domain Name System 94

Grüne IT COVER THEMA
Strategien für ein energieeffizientes Data Center 96

Projektarbeit
Document Driven Development mit dem Fit-Framework 102

WISSEN

Embedded Systems COVER THEMA
Individuelle Optimierung von Echtzeit-Anwendungen 106

Parallelisierung
Java in Multi-Core-Umgebungen 110

Multimedia
Aktuelle Techniken und Methoden fürs Media Streaming 114

Softwarearchitekturen
Systematisches Softwaredesign in der Nussschale 118

Single Sign-On COVER THEMA
Zentrales Sicherheits-informationssystem FreeIPA 122

Metadaten
Bildannotationen im semantischen Web 126

Schadsoftware COVER THEMA
Masseninfektionen mit Web Exploit Toolkits 131

PRAXIS

Tools und Tipps
Streaming mit dem VLC-Player 135

Active-Directory-Integration II COVER THEMA
Unix-Benutzerinformationen ins Active Directory migrieren 138

E-Mail
Variables Greylisting zur Spam-Abwehr 144

Java-Programmierung COVER THEMA
Assistenten bauen in Java: Die Wizard-API 150

MEDIEN

Internet-Infos
Comics als Abbild des Alltagslebens 154

Vor 10 Jahren
Vor 10 Jahren 155

Buchmarkt
Webentwicklung 156

Rezensionen
Softwareindustrie, PHP 5, Ruby on Rails 2 158

RUBRIKEN

Editorial 3
Leserbriefe 10
iX extra: Security nach Seite 130
Seminarkalender 160
Marktteil 161
Stellenmarkt 167
Impressum 176
Inserentenverzeichnis 177
Vorschau 178

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

Unterordner im Blackberry

(Smartphones: Business-Handys von RIM, HTC, Nokia und Apple, *iX* 10/08, S. 34)

In Ihrem Artikel schreiben Sie, dass Blackberry keine Unterordner und damit auch kein Verschieben von Emails in diese Ordner unterstützt. Dies ist nicht korrekt. Man muss nur über den BES-Administrator, den Desktop-Client oder über das Blackberry-Endgerät festlegen, welche Exchange-Ordner synchronisiert werden sollen. Standardmäßig ist dies leider wirklich nur der Posteingang. Nach Auswahl anderer Ordner wird deren Inhalt auf dem Blackberry angezeigt und Emails können auch verschoben werden.

CARSTEN MÜLLER, LANGGÖNS

Zu konservativ beurteilt

(Smartphones: Business-Handys von RIM, HTC, Nokia und Apple, *iX* 10/08, S. 34)

Für einen vergleichenden Test der aktuellen Smartphonetechniken bin ich immer dankbar, insbesondere weil dieser Test die Geräte einmal vom Aspekt der Usability aus betrachtet – ein Ansatz, der bei den üblichen Whitepaper-Attacken zu kurz kommt.

Das HTC Touch Diamond wird aus meiner Sicht allerdings zu sehr aus etwas zu konservativer Sicht betrachtet. Dieses Gerät hat in unserem Hause *(Landeshauptstadt Hannover, d. Red)* die Akzeptanz von Windows-Mobile-Smartphones deutlich erhöht. Es hat sich gezeigt, dass gerade der „Ich will doch nur telefonieren“-Anwender positiv darauf reagiert, wenn die wichtigsten Funktionen durch Fingertippen ohne Menüs und ohne Stiftbenutzung zu erreichen sind.

Auch sind einige Funktionen nicht richtig wiedergegeben:
– Die fingerbediente Kontaktliste akzeptiert natürlich auch Kontakte, für die kein Foto hinterlegt ist. Es werden mehrere Dummybilder (Scherenschnitte) angeboten, aus denen dann ausgewählt werden kann. Alternativ kann auch ein beliebiges auf dem Gerät gespeichertes Bild ausgewählt werden.
– Der Comm-Manager zum An- und Abschalten von Geräteschnittstellen muss nicht mit Schiebereglern bedient werden, man kann einfach auf jeden Eintrag wie „WLAN“ oder „Bluetooth“ mit dem Finger tippen und schaltet damit die Funktion an oder aus.
– Die Mailansicht im TouchFlo dient nur der Voransicht, man sieht auf einen Blick, wer geschrieben hat, und kann die erste Zeile der Mail lesen. Mit einmal Antippen der Mail landet man in der normalen Leseansicht. Diese Voransicht zeigt mir meist auf einen Blick, ob die Mail akut relevant ist oder noch bei besserer Gelegenheit gelesen und beantwortet werden kann. Die hinter der Mail beschriebene Listenansicht des Postfaches sieht man dagegen, indem man links unten auf Posteingang tippt.

DER DIREKTE DRAHT ZU iX

Redaktion iX
Postfach 61 04 07
30604 Hannover

Fax: 05 11/53 52-361
E-Mail: <user>@ix.de
Web: www.ix.de

Direktwahl zur Redaktion: 05 11/53 52-387

Für telefonische Anfragen zu Artikeln, technischen Problemen, Produkten et cetera steht die Redaktion wie gewohnt während der Lesersprechstunde zur Verfügung. Und zwar:

Montag bis Freitag, 11 bis 12 Uhr

Bitte nur während der genannten Zeiten anrufen und möglichst die angegebene Durchwahl benutzen.

<Durchwahl>	<user>	
-387	post	Redaktion allgemein
-377	avr	(André von Raison)
-590	ck	(Christian Kirsch)
-387	cle	(Carmen Lehmann)
-374	hb	(Henning Behme)
-379	jd	(Jürgen Diercks)
-386	js	(Jürgen Seeger)
-367	ka	(Kersten Auel)
-153	mm	(Michael Mentzel)
-787	mr	(Michael Riepe)
-373	rh	(Ralph Hülsenbusch)
-689	sun	(Susanne Nolte)
-368	un	(Bert Ungerer)
-535	ur	(Ute Roos)
-384	wm	(Wolfgang Möhle)

Listing-Service:
Sämtliche in *iX* seit 1990 veröffentlichten Listings sind über den iX-FTP-Server erhältlich:
ftp.heise.de/pub/ix/

iX-Link Bei Artikeln mit diesem Hinweis können Sie auf www.ix.de das zugehörige Argument (ixJJMMSSS) eingeben, um eine klickbare Liste aller URLs zu bekommen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Der Touch Diamond scheidet die Geister zugegebenermaßen: Stiftgewohnte Mitarbeiter nutzen teilweise auch weiter die gewohnte Bedienung. Für diese kann man mit wenigen Klicks die gewohnte klassische Oberfläche herstellen.

Was die Erfahrung in unserem Hause zeigte: Die im Gerät eingebaute Ausziehtastatur von Geräten wie dem Touch Pro, TyTn 2 (MDA Vario III) oder P4350 wird von einigen Nutzern nachgefragt, von den meisten aber nur in der ersten Gewöhnungsphase genutzt. Nach kurzer Zeit wird die Onscreentastatur per Stift oder Finger benutzt, die Auszugstastatur wird doch als ungewohnt und störend empfunden.

Was für den Test noch interessant gewesen wäre, ist eine Betrachtung der real zu erwartenden Laufzeiten bei normalem Gebrauch als Handy mit Pushmail. Die Akkulaufzeit eines Touch Diamond, die als reines Telefon über einer Woche liegt, sinkt mit Pushmailnutzung gerne auf 48 bis 60 Stunden. Beim iPhone scheint die Standzeit ähnlich zu sein, das Nokia- und das RIM-Gerät kann ich hier nicht einordnen.

DETLEV RACKOW, HANNOVER

Ordner im Nokia E71

(Smartphones: Business-Handys von RIM, HTC, Nokia und Apple, *iX* 10/08, S. 34)

Auf Seite 42 schreibt Herr Kirsch: „Als einziger im Test erlaubt er [der HTC Touch Diamond] das Abonnieren von Ordnern.“ Das ist nicht korrekt. Der E-Mail-Client des Nokia E71 erlaubt ebenfalls das Abonnement von Ordnern. Hier widerspricht sich Herr Kirsch auch selbst, da er auf Seite 40 noch schreibt:

„IMAP-Folder lassen sich zwar abonnieren und relativ normal bearbeiten […]“

Im Artikel vermisse ich im Übrigen auch eine Gegenüberstellung der VoIP-Funktionalität. Mir ist nicht klar, warum der Autor die SIP-Clients (falls vorhanden) nicht verglichen hat bzw. überhaupt gar nicht angesprochen hat.

So wirklich gelungen ist der Artikel nicht, da es dem Autor meiner Meinung nach nicht gelungen ist, einen gemeinsamen Nenner für einen qualitativ ansprechenden Vergleich der vier Smartphones zu finden.

DANIEL PHILIPP, STUTTGART

Schöner Überblick

(Client-Management: Marktübersicht PC-Management-Software, *iX* 10/08, S. 80)

Ihr Artikel ist ein sehr schöner Überblick, der die Probleme bei der Einführung von solchen Systemen gerade im Mittelstand gut beschreibt. Schade nur, dass das Opensource Desktop Managementsystem „opsi“ keine Erwähnung gefunden hat. Zumal gerade dieses Produkt bei mittelständischen Betrieben (nicht zuletzt aus preislichen Gründen) gut angenommen wird.

DETLEF OERTEL, MAINZ

Offene Systeme totgeschwiegen

(Embedded Systems: Betriebssysteme, *iX* 10/08, nach S. 146)

Das extra enttäuscht mich zutiefst. Offensichtlich von den Anzeigenkunden getrieben, werden nur kommerzielle eingebettete Betriebssysteme gelistet und offene System wie eCos, uCLinux und RTEMS einfach totgeschwiegen.

Gerade letzteres hätte Erwähnung verdient, da es als einziges eine komplette ADA-Unterstützung bietet und außerdem so robust und gereift ist, dass es bei DESY, CERN, ESA und NASA (Dawn mission, framing camera) zum Einsatz kommt.

WOLFRAM WADEPOHL, REUTLINGEN-OHMENHAUSEN

In der Tat ist die Liste nicht vollständig, weil die schiere Menge der Betriebssysteme im Embedded-Umfeld eine komplette Auflistung nicht zulässt. Leider ist der Hinweis auf die Beschränkung auf kommerzielle Betriebssysteme der Schere zum Opfer gefallen. Interessierte können wir an dieser Stelle nur auf iX extra 2/09 vertrösten, das unter dem Thema „Industrie-PCs und ihre Betriebssysteme“ auch die Open-Source-Varianten vorstellt. *(d. Red.)*

Anzeige

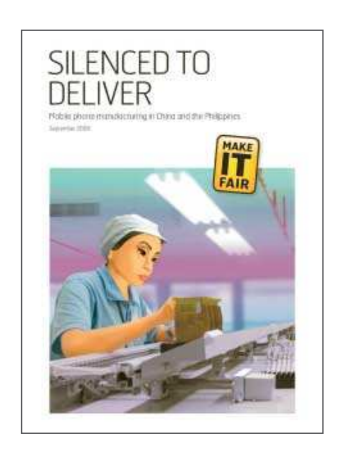
Die *iX*-Redaktion behält sich Kürzungen und auszugsweise Wiedergabe der Leserbriefe vor. Die abgedruckten Zuschriften geben ausschließlich die Meinung des Einsenders wieder, nicht die der Redaktion.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

Handyproduktion unter harten Bedingungen

Einer Studie der von der EU finanzierten Organisation MakeITFair zufolge genügen die Arbeitsbedingungen in vielen asiatischen Handyfabriken weiterhin nicht den internationalen Vorgaben und lokalen Gesetzen. Die Untersuchung (s. *iX*-Link) betrachtete vier chinesische und zwei philippinische Produktionsstätten. Zwar würden dort die Mindestlöhne gezahlt, sie reichten jedoch häufig nicht zum Leben. So erhalte ein Arbeiter in einer Exportzone auf den Philippinen 120 € monatlich, eine Familie benötige jedoch 200 € mehr. Die unzureichende Entlohnung erhöhe die Bereitschaft, Überstunden zu leisten. In Spitzenzeiten komme es so zu Wochenarbeitszeiten von 80 Stunden; alle untersuchten chinesischen Fabriken hätten die gesetzlich vorgeschriebene Maximalzahl von 36 Überstunden pro Woche überschritten. Weitere Kritikpunkte betreffen Strafzahlungen, die die Unternehmen von den Löhnen einbehalten, und die Gesundheitsbedingungen. So werde wegen des Zeitdrucks



häufig ohne die vorgeschriebene Schutzkleidung mit gefährlichen Chemikalien gearbeitet.

China produziert zurzeit rund 250 Millionen Handys jährlich, die Hälfte aller weltweit hergestellten Geräte. Auftraggeber der untersuchten Fabriken sind Motorola, Nokia, Sony-Ericsson, Apple, LG und Samsung. Die beiden Letzteren verweigerten Kommentare zu der Studie; die übrigen Firmen wollen die Kontrolle der Arbeitsbedingungen verbessern.

iX-Link ix0811012

Kaspersky sieht Handyviren kommen

Nach Auffassung der russischen Anti-Viren-Firma Kaspersky nutzen Virenautoren vermehrt den als „write once, run everywhere“ beworbenen Vorzug von Java-Programmen: Sie laufen unverändert auf jeder Plattform, die eine passende virtuelle Maschine bereitstellt. Diese Voraussetzung erfüllen mittlerweile viele Handys, auf denen die Java Micro Edition (J2ME) installiert ist.

Ziel der Malware sei es, SMS-Nachrichten an kostenpflichtige Dienste zu senden. Nach eigenen Angaben hat Kaspersky bereits 50 solche Programme entdeckt. Damit habe sich gegenüber dem zweiten Halbjahr 2007 die Zahl vervierfacht. Allerdings warnen die Hersteller von Anti-Viren-Programmen seit Jahren vor Handyviren – bislang gab es jedoch noch keines, das sich nennenswert verbreitet hätte.

Aus für Nokias Intellisync

Nur knapp drei Jahre, nachdem Nokia Intellisync und dessen gleichnamige Synchronisierungssoftware übernommen hatte, kam das Aus: Der Handyhersteller wird das Paket aus Mobile Suite, Wireless E-Mail, Device Management und Application Sync seinen Unternehmenskunden nicht mehr als eigenständiges Produkt anbieten. Nur auf dem eigenen Ovi-Portal soll Intellisync noch laufen. Vorhandene Installationen will Nokia noch für zwei Jahre warten und in dieser Zeit beim Umstieg auf andere Produkte helfen.

In Zukunft sollen die hauseigenen S60-Handys das Activesync-Protokoll nutzen, das unter anderem der Exchange-Server verwendet. Auch mit IBM und Cisco will Nokia stärker zusammenarbeiten. IBM deutete an, dass sein Domino 8.5 den „Lotus Traveler“ enthalten und S60-Geräte unterstützen werde.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Adobe bringt Creative Suite 4

Adobe hat eine Neuauflage seiner Creative Suite vorgestellt. Es gibt nicht nur neue (CS4-)Versionen der einzelnen Anwendungen wie Photoshop, Indesign, Illustrator, After Effects, Premiere Pro, Dreamweaver und Flash Professional, sondern auch insgesamt sechs neue Creative-Suite-4-Editionen für verschiedene Anwendungsschwerpunkte.

Die Adobe Creative Suite 4 Design Premium enthält Anwendungen für das Design in Print, Web und für mobile Geräte. Das sind im Einzelnen: Adobe Indesign CS4, Photoshop CS4 Extended, Illustrator CS4, Flash CS4 Professional, Dreamweaver CS4, Acrobat 9 Pro sowie das neu hinzugekommene Adobe Fireworks CS4 für das schnelle Entwerfen von Website-Prototypen.

Die Creative Suite 4 Web Premium ist – wie der Name schon sagt – für Webdesign optimiert. Sie enthält kein Indesign, dafür aber zusätzlich Adobe Contribute CS4, Device Central CS4 und die Audiobearbeitungssoftware Adobe Soundbooth CS4.

Adobe Creative Suite 4 Production Premium schließlich ist die Komplettlösung für Kreativprofis zur Erstellung von Video-, Audio- und interaktiven Inhalten für die Nutzung im Web, auf mobilen Endgeräten und zur TV-Ausstrahlung. Die Creative Suite 4 Production Premium enthält die neuen Versionen von Adobes Video-, Audio-, Web- und Design-Lösungen Adobe After Effects CS4 Professional, Premiere Pro CS4, Encore CS4, Photoshop CS4 Extended, Illustrator CS4, Flash CS4 Professional, Soundbooth CS4 und Onlocation CS4, das jetzt auch die native Unterstützung für Intel-Macs bietet.

Neu in der Version 4 der Creative Suite ist vor allem der noch größere Stellenwert, den Flash einnimmt. Zum Beispiel kann die Designerin ein Layout in Indesign mit den interaktiven Gestaltungsmöglichkeiten von Flash CS4 Professional verbinden, indem sie das Indesign-Dokument als XFL-Datei exportiert und dann in Flash CS4 Professional öffnet, um Interaktionen, Animationen und Navigationsmöglichkeiten zu ergänzen. Auf diese Weise ist die praktisch nahtlose Gestaltung interaktiver Broschüren, dynamischer Präsentationen und von Online-Publikationen möglich, indem Seitenübergänge, interaktive Schaltflächen und Links zu einem Dokument hinzugefügt werden. Das lässt sich dann als SWF-Datei für die Wiedergabe im Adobe Flash Player oder als interaktive PDF-Datei exportieren.

Dieter Michel

iX-Umfrage: Google-Skepsis überwiegt

Nur eine kleine Minderheit von 12 Prozent steht den Plänen Googles, einen eigenen Webbrowser herauszubringen, aufgeschlossen gegenüber. So zumindest das Ergebnis der Umfrage, die parallel zu Ausgabe 10/08 auf www.ix.de lief. Von diesen 12 % geht es den meisten auch um den Wunsch nach Konkurrenz für Microsoft. Immerhin 10 % der Antwortenden machen ihre Entscheidung von der Qualität des Browsers Chrome abhängig, mehr als drei Viertel haben Bedenken wegen der Monopolstellung oder des Datenschutzgebarens des Suchmaschinengiganten. Die genaue Fragestellung zeigt die Grafik.

Bei der nächsten Umfrage, die mit Erscheinen dieses Heftes startet, geht es um Outsourcing.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Kontron kauft Intels Telko-Server-Sparte

Zu einem nicht genannten Preis wird Intel seine Abteilung für Telekommunikationsserver an seinen bisherigen Kooperationspartner Kontron abtreten. Teil des sogenannten Asset Deals, bei dem ein Unternehmen alle Wirtschaftsgüter eines anderen erwirbt, sind die Fertigungsanlagen in Columbia (South Carolina) und im malaysischen Penang, die zusammen etwa 70 Angestellte beschäftigen.

Der Echinger Spezialist für Embedded Systems und Industrie-DV fertigt bereits AdvancedTCA- und MicroTCA-Blades (Telecom Computing Architecture) für die Telekommunikations-Branche und will mit den „Carrier Grade“ Rackmount-Servern sein Portfolio abrunden. Nach Schätzungen von Kontron soll der neue Geschäftsbereich im nächsten Jahr einen Umsatz von 40 Millionen US-Dollar erzielen. *Axel Urbanski*

iX-Link ix0811014

Kompakter Industrie-PC unter Linux

Nur 12 × 10 × 4 cm^3 und etwa 380 g schwer ist die Tiny Box TB5200L von TQ-Components (www.tq-components.com). Herz des kleinen Industrie-PCs ist ein MPC5200-Prozessor von Freescale, der laut Hersteller bei einem Takt von 400 MHz eine Rechenleistung von 760 MIPS bietet. Das Gerät verfügt über maximal 128 MByte SDRAM und 32 MByte Flash-Speicher. Ein Compact-Flash-Steckplatz erlaubt den Anschluss von bis zu 64 GByte zusätzlichem Massenspeicher.

Neben je zwei seriellen und CAN-Bus-Schnittstellen bietet die Tiny Box zwei USB-Hostports (USB 1.1) und Ethernet (siehe Abbildung). Die externe Stromversorgung muss 15 bis 30 V Gleichspannung und eine maximale Leistung von 10 W liefern. Als Standardbetriebssystem bietet der Hersteller Linux mit einem 2.6er Kernel an; auf Anfrage ist das Gerät auch mit dem SPS-Betriebssystem CoDeSys (Controller Development System) erhältlich.





Quelle: TQ-Components

Mini-Pinguin: Die Tiny Box TB5200L von TQ-Components läuft standardmäßig unter Linux.

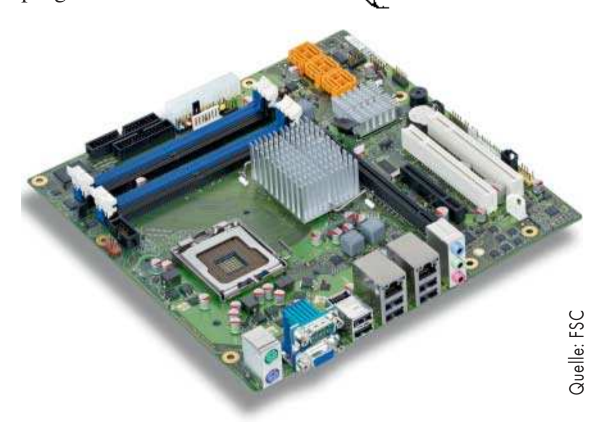
Neue Industrie-Mainboards von FSC

Um zwei neue Mitglieder erweitert Fujitsu-Siemens sein Angebot an Industrie-Mainboards: das D2831-S im Micro-ATX-Format und das ATX-Board D2836-S. Beide eignen sich für den Dauerbetrieb bei Temperaturen zwischen 0 und 60 °C. Als Basis dient Intels Q45-Express-Chipsatz, der mit den Prozessoren Core 2 Duo und Core 2 Quad zusammenarbeitet. Vier Speichersockel nehmen maximal 16 GByte DDR2-800-SDRAM auf.

Zur Standardausrüstung gehören unter anderem zwei Gigabit-Ethernet-Buchsen, sechs SATA-II-Ports, ein Floppy-Interface, ein serieller Port, HD-Audio sowie PS/2-kompatible Anschlüsse für Tastatur und Maus. Der integrierte Management-Controller beherrscht das Alert Standards Format (ASF 2.0) und bietet neben den üblichen Überwachungsfunktionen die Möglichkeit, eine individuelle Lüfterregelung zu programmieren.

Leider besitzt die DirectX-10-fähige Onboard-Grafik nur einen VGA-Ausgang. Sechs USB-Buchsen sind von außen zugänglich. Intern stehen zwei weitere bereit, etwa für ein Lizenz-Dongle oder einen Flash-Speicher mit dem Betriebssystem. Zwei weitere USB-Anschlüsse sind als Stiftleisten ausgeführt. Das Micro-ATX-Board D2831-S (siehe Abbildung unten) stellt einen PCI-Express-Slot mit 16 Lanes und doppelter Geschwindigkeit (PCIe 2.0), einen PCIe-4x-Slot sowie zwei 32 Bit breite PCI-Steckplätze zur Verfügung. Beim D2836-S kann der Entwickler zwei weitere PCI-Slots und einen dritten PCIe-Steckplatz (1x) für Erweiterungen nutzen. Muster beider Boards sind bereits verfügbar, die Serienproduktion des D2836-S soll Anfang November beginnen, die des D2831-S Ende November. *Axel Urbanski*

iX-Link ix0811014



Quelle: FSC

Strapazierfähig: Industrie-Mainboards wie das Micro-ATX-Board D2831-S von Fujitsu-Siemens halten erheblich mehr aus als normale Server-Boards.

Atom N270 als Embedded-CPU

Intel hat den Atom-Prozessor N270 und den dazu passenden Mobile Intel 945GSE Express Chipset in seine Embedded-Roadmap aufgenommen. Damit garantiert der Hersteller, dass die aus Netbooks bekannten Chips (siehe den Artikel „Winzigkeiten“ auf Seite 54) mindestens sieben Jahre lang lieferbar bleiben. Entwickler haben nun die Wahl zwischen beiden Varianten des Atom: dem Diamondville (N270) und dem kompakteren Silverthorne (Z5xx-Familie).

Ersteren verwendet Kontron (de.kontron.com) auf seinem frisch angekündigten ETX-DC 3.0 Computer-on-Module. Das mit Version 3 des ETX-Standards (Embedded Technology eXtended) der EXT Industrial Group (www.ext-ig.com) kompatible Board misst lediglich 95 × 114 mm^2 und lässt sich einfach in die Schaltung des Kunden einstecken. Dank seiner geringen Leistungsaufnahme von maximal 12 bis 15 W lässt es sich mit passiver Kühlung und in vollständig geschlossenen Gehäusen betreiben.

Den Löwenanteil von 6 W gönnt sich der Intel 82945GSE Graphics Memory Controller. Eine maximale Auflösung von 2048 × 1536 Pixeln, ein LVDS-Anschluss für LCD-Panels mit 1600 × 1200 Pixeln, ein TV-Ausgang für HD-Auflösung und Dual-Monitor-Betrieb rechtfertigen jedoch seinen Energiehunger. Außerdem kann das Board mit High Definition Audio und – optional – einem Trusted Platform Module (TPM 1.2) aufwarten. Neben den vom ETX-Standard geforderten Schnittstellen wie ISA, PCI und USB 2.0 findet sich auf der Platine ein AHCI-kompatibler SATA-II-Controller mit zwei Ports. Als Betriebssystem lassen sich Windows Vista, XP, XP Embedded und CE sowie Linux und VxWorks einsetzen. *Axel Urbanski*

iX-Link ix0811014

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

eco-Kongress 2008

Bunt gemischt

Achim Born

„Beyond the Borders“ überschrieb der eco-Verband seinen diesjährigen Kongress. Der Slogan war etwas zu hoch gegriffen, da die Vorträge eigentlich keine Grenze sprengten. Dafür bekamen die Teilnehmer jedoch einen Eindruck davon, was Internetprovider & Co. derzeit bewegt.

Wenn Ressourcen nicht mehr grenzenlos zur Verfügung stehen, bewegt sich das nachhaltige Haushalten auf der Prioritätenliste aufwärts. Den Auftakt des eco-Kongresses 2008 bildeten daher vor über 100 Teilnehmern die heutigen Anforderungen an Rechenzentren und Infrastruktur. Zu Beginn referierte Dieter Schramm, bei Dell in der Service-Sparte tätig, über das Rechenzentrum der Zukunft. Sein naturgemäß nicht herstellerneutrales Credo lautet „Simplify IT“ als Ansatz für eine effizientere IT. In Beispielrechnungen führte der Dell-Mann vor, wie sich das Verhältnis Gesamtstromverbrauch zu Verbrauch durch IT (aktuell: 3,3 : 1) reduzieren lässt.

Dabei plädierte Schramm aus Effizienzgründen unter anderem für die Versorgung der Rechner in den Rechenzentren mit Gleichstrom, diskutierte des Weiteren die bessere Trennung kalter und warmer Luftströme nach dem Prinzip der freien Kühlung sowie Virtualisierung, um schon die Zahl der Rechner zu verringern. Eine Standardlösung, die zu allen Organisationen passt, konnte Schramm aber nicht nennen. Deshalb behalf er sich mit einem Allgemeinplatz und empfahl, die Energieeffizienz zum Bestandteil der IT-Strategie zu machen.

Die vom Dell-Mann grob skizzierten Gedanken zur Kühlung führte Gerhard Leo Büttner, Chef des Design Institut München, ausführlich und kompetent aus. Über 40 Jahre Erfahrung im RZ-Design und mehr als 400 Projekte belegen, dass er weiß, wovon er spricht. Ausführlich ging er auf die Prinzipien der freien Kühlung und der Brennstoffzelle ein. Unterhalb einer Außentemperatur von 14 °C und bei entsprechender Auslegung des Freikühlregisters lässt sich das Kühlwasser ohne Einsatz der Kältemaschine so weit kühlen, dass es die angestrebten Raumkonditionen (22 °C, 50 % rel. Luftfeuchtigkeit) gewährleistet. Das bedeutet eine Energieeinsparung von bis zu 70 %.

Darüber hinaus lassen sich echte „Minderkosten“ mittels Wärmerückgewinnung erzielen, falls ganzjährig Niedertemperaturverbraucher wie Heizung, Schwimmbad et cetera als Abnehmer zur Verfügung stehen. Zu beachten ist in jeden Fall der Verfügbarkeitsaspekt. Denn so gut Brunnen für die Kühlung prinzipiell geeignet sind, bedarf es eines Reservesystems, wenn der Wasserspiegel zu stark fällt.

Mangelware IPv4-Adressen

Auf einen ganz anderen „Verbrauchsaspekt“ machte Frank Orlowski, Director Business Development beim DE-CIX, mit Blick auf die Ressourcen aufmerksam. Entgegen der weitverbreiteten Meinung drohe dem Internet weniger ein Engpass aufgrund des exponentiell wachsenden Verkehrs, dem die Investitionen im Netz nur linear folgen. Das eigentliche Problem verursache der begrenzte IPv4-Adressraum. Am 29. September 2012 sei er aufgebraucht, werde die aktuelle Entwicklung fortgeschrieben. Mit IPv6 sei die Rettung seit geraumer Zeit verfügbar. Allerdings nutze kaum jemand unter den Providern das neue Internetprotokoll. „Die meisten Provider wirken angesichts des zur Neige gehenden Adressraums recht unbekümmert“, bemerkte der DE-CIX-Manager. Anscheinend fehle echter Leidensdruck. Falls die Provider diese Haltung nicht ablegen, rechnet Orlowski im schlimmsten Fall sogar damit, dass Unternehmen allein aufgrund ihres Adressraums akquiriert sowie deren Adressen versteigert werden.

Im Rahmen der eco-Tagung durften acht Jungunternehmen ihre Geschäftsideen vorstellen. Die Präsentation erfolgte in der kurzweiligen Form des „Elevator Pitch“: Die Vortragenden hatten nur vier Minuten Zeit für ihre Vorstellung. Beginnen durfte Hiogi (hiogi.de) mit ihrer Frage-/Antwort-Community auf SMS-Basis. Es folgte realisr.com, eine offene Plattform für die Erstellung individueller „Corporate Communities“ sowie Kampagnen-Portale. Weiter ging’s mit dem im Juli gestarteten Studijob24.de, einer Jobbörse, die Familien und Unternehmen mit fachkundigen Studenten zusammenbringt, aber auch so simple Tätigkeiten wie Babysitting vermittelt. Hinter Jimbo (de.jimdo.com), das mit den Samwer-Brüdern und United Internet über prominente Geldgeber verfügt, steckt ein Baukastensystem zum Erstellen eigener Homepages. Juipidi (www.jupidi.de) erweitert wiederum die boomende Phalanx der webbasierenden Kontexttools. Der mobile Flirtingdienst will das altmodische Zettelschreiben ablösen und verknallten Teenies anonym die Kontaktaufnahme per SMS erleichtern. Townkings.de soll dagegen Gleichgesinnte einer Nachbarschaft zusammenbringen. Mindmeister (www.mindmeister.com) ist letztlich ein gehosteter Service für „Mind Maps“, grafische Darstellungen von Gedanken und Ideen.

Den Abschluss bildete Qitera (www.qitera.com). Mit dem Dienst lassen sich per Klick die für den Nutzer wichtigen Dinge (Website, Video oder Produkte) im Internet sicher speichern und sich mit Personen, denen man den Zugriff einräumt, teilen. Ob einer der acht Unternehmungen tatsächlich die Aufzugfahrt zum großen Geld winkt, sei dahingestellt. Jedenfalls gaben die Vortragenden einen interessanten Überblick über aktuelle Ideen rund um Web und Communities.

Am Gelde hängt doch alles

Meldungen zur Finanzkrise und zum Zusammenbruch des Kreditmarktes füllen zurzeit die Gazetten. In Sachen (Video-) Content herrscht schon längere Zeit pekuniärer Mangel. Zumindest beklagte dies Ibrahim Evsan: „Zukunftsträchtige Entwicklungen verlagern sich aufgrund der mangelnden Investitionsbereitschaft nach Amerika. Diese Entwicklung finde ich nicht nur sehr traurig, sondern auch gefährlich“, so der Sevenload-Chef. In seinem Vortrag zum Thema Web-TV malte er ein wenig erfreuliches Bild von der Zukunft der hiesigen Branche. Denn die fehlende finanzielle Untermauerung der Infrastrukturanbieter hierzulande geht einher mit den wachsenden Qualitätsansprüchen der Anwender. Verfahren wie HDTV bedeuten jedoch für Anbieter, dass sich der Bedarf an Übertragungs- und Serverkapazität verdoppelt.

Content versus Kosten

Bedauerlicherweise interessieren die Kosten auf Provider-Seite den Anwender wenig, obgleich er vermehrt auf das Video im Internet zurückgreift. Evsan kann da nur neidvoll auf die USA verweisen, wo noch Investoren unterwegs sind. Ein wenig Hoffnung setzt er in Refinanzierung via Werbeeinnahmen, wie er auf der abschließenden Podiumsdiskussion ausführte. Auch seine Mitdiskutanten frönen dem Prinzip Hoffnung, dass guter Content auch im Web 2.0 den Nutzern einige Cents wert sein sollte. (un)

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

iX-Veranstaltungen

www.ix-konferenz.de.

Gleich drei „Calls for Papers“ gehen mit Erscheinen dieser Ausgabe online. Zum einen startet der Aufruf zum Einreichen von Vorträgen für das **Cebit Forum Software & Systems 2009**. Denn auch im nächsten Jahr findet wieder die weltgrößte IT-Messe in Hannover statt, und zwar vom 3. bis 8. März. Das *iX* Cebit Forum präsentiert sich im neuen Gewand und mit Unterausstellern, Details finden Sie auf unserer Konferenz-Website.

Der zweite CfP betrifft die Konferenz zur **IPv6-Einführung**, die am 29. Mai in Frankfurt/M. stattfindet, mit Tutorials am Vortag. Es handelt sich dabei um eine Kooperationsveranstaltung mit heise Netze; gesucht werden herstellerunabhängige, neutrale Vorträge (keine Werbung). Es sind ausdrücklich nicht nur „Success Stories“, sondern auch Darstellungen von negativen Aspekten oder gescheiterten Projekten erwünscht.

Last but not least findet vom 5. bis 7. Mai 2009 in München wieder die **Teamconf** statt, die Konferenz zum Thema Visual Studio Team Systems, veranstaltet in Zusammenarbeit mit HLMC. Wer dazu einen Vortrag einreichen möchte – der CfP ist eröffnet.

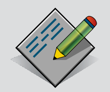
Zwei Monate früher geht es um ein anderes Thema: Angriffe auf Webanwendungen häufen sich, und wirksame Schutzmaßnahmen dagegen sind alles andere als trivial. Helfen kann ein Besuch des dreitägigen Seminars **Angriffe auf Web-Applikationen**, das *iX* zusammen mit den Sicherheitsspezialisten von Cirosec veranstaltet – 17. bis 19. März in Frankfurt/M.

Noch einen Monat früher geht es in Essen wieder los: Am 3. Februar starten neue Windows-Powershell-Seminare – drei Tage zu Microsofts mächtigem Kommandozeilenwerkzeug mit Peter Monadjemi und Holger Schwichtenberg.

Und auch in diesem Jahr sind noch kurzfristig einige Veranstaltungen angesetzt worden. Wegen des großen Zuspruchs auf seine Keynote auf der MedConf 2008 hält Prof. Dr. Christian Johner am 16./17. Dezember 2008 in Freiburg ein zweitägiges Seminar ab zum Thema **Medizinische Software gesetzeskonform entwickeln**. Ebenfalls auf der MedConf entstanden ist der am 16. Dezember in Hamburg angesetzte Workshop **Einsatz von modernen SW-Entwicklungspraktiken in der Medizintechnik**.

Ein Abkömmling der TeamConf wiederum sind die Eintagesveranstaltungen mit Neno Loje, **Einsteiger-Workshops** zum Thema **Visual Studio Team System und Team Foundation Server** in München (5.11.), Zürich (1.12.) und Frankfurt/Main (17.12.). Details dazu auf www.ix-konferenz.de und www.hlmc.de.

KURZ NOTIERT



Ausgebaut: Der Attachmate-Geschäftsbereich NetIQ dehnt seine VoIP-Management-Lösung auf den Microsoft Office Communications Server 2007 aus. Das Modul unterstützt das vollständige Management der VoIP-Nutzung mit der Kommunikationssoftware.

Eingebunden: Produkte von Foundry Networks sind künftig standardmäßig auf die Unterstützung von IBMs Tivoli-Netcool-Software vorbereitet. Die Partnerschaft zwischen beiden Firmen ermöglicht, dass die Netzwerkmanagement-Software die Alarme der Switches und Router von Foundry in Netcool/Omlnibus überwacht.

Leichte Zunahme: In den ersten acht Monaten dieses Jahres wurden knapp 20 000 IT-Stellen ausgeschrieben, sechs Prozent mehr als 2007. Das ermittelte der Personaldienstleister Adecco in seiner regelmäßigen Stellenmarktanalyse, in die IT-Jobangebote in 40 Tageszeitungen und der Computerwoche einflossen.

Onlineradio: On demand statt live

Einblicke in die Pläne der Deutschen Welle im Bereich Internet und Web 2.0 gab Holger Hank, Leiter Neue Medien bei dem traditionsreichen Funkhaus, auf dem eco-Kongress. Ungeachtet der Sensibilisierung der Kollegen für die neuen technischen Möglichkeiten postulierte er das Zusammenwachsen von Radio und Internet. Bei der digitalen Mediennutzung liegen zurzeit Podcasts vorn. Live-Streams machen den Ausführungen Hanks zufolge bei der Nutzung des Onlineangebots der Deutschen Welle nur noch einen ganz kleinen Part aus. Den Großteil des Datenverkehrs verursachen inzwischen On-Demand-Downloads. Deswegen werde der Live-Anteil im Radio heruntergefahren, da die Zukunft dem On-Demand gehöre.

Vorratsdatenspeicherung abgewehrt

Ein TK-Anbieter hat vor dem Verwaltungsgericht Berlin Klage gegen die Einführung der Vorratsdatenspeicherung eingelegt. Er trug vor, dass die Art und Weise der Umsetzung dieser Pflicht zur sechsmonatigen Speicherung von Telefon- und Internetdaten „unverhältnismäßig und verfassungswidrig“ sei. Insbesondere weil die Anbieter nach dem Gesetz keine Aufwandsentschädigung verlangen können, sei die gesetzliche Regelung rechtswidrig. Die Verwaltungsrichter werden das Gesetz nun voraussichtlich ans Bundesverfassungsgericht zur Klärung dieser Rechtsfragen weiterleiten. Solange es von dort keine Entscheidung gibt, wird der klagende Anbieter wohl zunächst von der Verpflichtung zur Vorratsdatenspeicherung befreit.

Tobias Haar

Kein Schutz gegen illegale Downloads

„Hilfssheriff Provider“ lautete der Titel einer Vortragsreihe auf dem eco-Kongress zum Thema „Recht und Regularien“. Stefan Michalk, Geschäftsführer des Bundesverbandes Musikindustrie, durfte an dieser Stelle für den fairen Ausgleich zwischen Kultur und Technik werben. 3,35 Mio. Personen hätten hierzulande im vergangenen Jahr mehr als 3,3 Mio. Songs illegal heruntergeladen. Als Gegenmittel bewarb er das Modell der „abgestuften Erwiderung“, wie es unter anderem in Frankreich Gesetz werden soll.

Potenzielle Konsequenzen für Unbelehrbare nannte Michalk indes nicht. Dagegen warb er um die Gunst der Provider. Denn auch sie würden vom Wegfall illegaler Downloads profitieren, da sich die Kosten für den Netzausbau verringerten, mehr Bandbreite für lukrative Pay-Angebote zur Verfügung stünde und eigene Onlineshops (etwa Musicload) gestärkt würden. In der abschließenden Diskussionsrunde wurde indes deutlich, dass sich die Provider mit diesem Speck nicht so einfach ködern lassen. So nannte Oliver J. Süme vom eco-Vorstand das vorgeschlagene Warnhinweismodell aberwitzig und datenschutzrechtlich problematisch. Volker Grassmuck von der Berliner Humboldt-Universität bemerkte, bei stärkerem Druck würde vermutlich als Gegenwehr auch die Verschlüsselung zunehmen.

Der Medienwissenschaftler hatte zuvor als neues Verwertungsmodell eine Content- oder Kultur-Flatrate vorgestellt, was so manchen Teilnehmer doch stark an eine zweite Rundfunkgebühr erinnerte. Letztlich zeigten sowohl die Podiumsdiskussion als auch die Vorträge, dass keine tragfähige Lösung in Sicht ist. Es gibt vermutlich auch keine, solange die Musikindustrie beinhart am Geschäftsmodell des CD-Verkaufs festhält. Letztlich wird sich aber auch die Musikindustrie der Tatsache stellen müssen, dass sie erst durch Technik möglich wurde und nun durch Technik wieder abgelöst wird. Online-Musikflatrates oder Apples Erfolg mit iTunes zeigen, dass es auch anders geht.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Gerichte uneins über Auskunftsanspruch

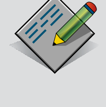
Seit September 2008 müssen Internetprovider auf Anfragen von Rechtsinhabern den hinter einer IP-Adresse steckenden Internetnutzer benennen, wenn ein Urheberrechtsverstoß in „gewerblichem Ausmaß“ vorliegt. Wann ein Verstoß gewerblich sein soll, hat das Gesetz ausdrücklich offen gelassen und der Rechtsprechung überlassen. Klar ist nur, dass sich dies nicht nur aus der Anzahl der Rechtsverletzungen, sondern auch aus deren Schwere ergeben kann. Jetzt liegen die ersten Gerichtsentscheidungen vor.

Das Landgericht Frankenthal (Az. 6 O 325/08) sieht erst ab rund 3000 Musiktiteln oder 200 Filmtiteln ein gewerbliches Ausmaß. Die Richter orientieren sich an den Leitlinien deutscher Generalstaatsanwaltschaften, die strafrechtliche Ermittlungen erst bei diesen Zahlen vorsehen. Demgegenüber haben die Richter an den Landgerichten Köln (Az. 28 AR 4-08) und Düsseldorf (Az. 12 O 425/08) einen Auskunftsanspruch bereits bei nur einem Album als gegeben angesehen. Auch die Kammern der Landgerichte Bielefeld (Az. 4 O 328/08), Oldenburg (Az. 5 O 2421/08), Frankfurt/M. (Az. 2-06 O 534/08) und Nürnberg (Az. 3 O 8013/08) lassen ein Album oder ein Hörbuch genügen. In Oldenburg reichte sogar die einfache Nutzung einer Tauschbörse. Ob hier bereits eine „gewerbliche“ Tätigkeit vorliegt, ist auf den ersten Blick doch sehr fraglich. Wie so oft wird sich diese unsägliche Rechtsunsicherheit aber erst dann auflösen, wenn die höchsten deutschen Gerichte darüber entscheiden. *Tobias Haar*

Mehr juristisches Unheil für Rapidshare

Das Hanseatische Oberlandesgericht hat sich in einem mittlerweile rechtskräftigen Urteil (Az. 5 U 73/07) in deutlichen Worten mit den Schwierigkeiten von Rapidshare beim Einhalten der Urhebergesetze auseinandergesetzt. „Ein Geschäftsmodell, das aufgrund seiner Struktur durch die Möglichkeit des anonymen Hochladens in Pakete zerlegter, gepackter und mit Kennwort gegen den Zugriff geschützter Dateien der massenhaften Begehung von Urheberrechtsverletzungen wissentlich Vorschub leistet, kann von der Rechtsordnung nicht gebilligt werden“, so die Richter in seltener Eindeutigkeit. Die Betreiber von Rapidshare können sich auch nicht auf etwaige Erleichterungen bei der Prüfungspflicht rechtswidriger Inhalte berufen, wenn „der Betreiber ihm zumutbare und nahe liegende Möglichkeiten, die Identität des Nutzers zum Nachweis einer etwaigen Wiederholungshandlung festzustellen, willentlich und systematisch ungenutzt lässt“. *Tobias Haar*

KURZ NOTIERT



Schweiz billiger: Die Eidgenössische Kommunikationskommission (ComCom) hat eine Senkung der Preise verfügt, die Swisscom von ihren Wettbewerbern verlangen darf. Statt 23,50 Franken darf sie künftig nur noch 18,18 Franken pro Monat für die „letzte Meile“ abrechnen.

Weniger Vorrat: Kleine Hotspot-Betreiber sind von der Vorratsdatenspeicherung befreit. Die Bundesregierung sieht keine Speicherpflicht „für private Anbieter öffentlicher WLAN-Zugänge sowie für Kleinbetriebe“ vor. Die Grenze zwischen diesen und protokollpflichtigen Anbietern ist derzeit aber noch unklar.

Markenverletzung per Umleitung: Wer eine fremde Marke als Domain verwendet, begeht auch dann eine Markenverletzung, wenn dort nur ein „Redirect“ auf eine andere Domain startet (Oberlandesgericht Hamburg, Az. 5 W 102/07).

E-Mail-Adresse allein genügt nicht

Der Bundesgerichtshof (Az. I ZR 197/05) hat entschieden, dass niemand davon ausgehen darf, dass ein E-Mail-Nutzer mit dem Erhalt von Werbemails einverstanden ist, nur weil er seine Adresse auf einer Webseite veröffentlicht. Gehen dennoch solche E-Mails an diese Adresse, liegt ein rechtswidriges Spamming vor. In der Veröffentlichung der Adresse liegt kein „stillschweigendes Einverständnis“, Werbung zu erhalten. Sie dient vorrangig – für jeden erkennbar – der Kontaktaufnahme mit dem Betreiber der Webseite und ist insbesondere im Impressum vorgeschrieben. *Tobias Haar*

Abkommen gegen Produktpiraterie

Von der Öffentlichkeit bislang kaum wahrgenommen, diskutieren die Industrieländer derzeit über ein internationales „Anti-Counterfeiting Trade Agreement“ (ACTA). Ziel dieses Übereinkommens soll die Schaffung eines effizienten und sicheren Rechtsrahmens für die Bekämpfung von Produktpiraterie sein. Die Beratungen finden unter Ausschluss der Öffentlichkeit statt, was zivilgesellschaftliche Organisationen aus aller Welt als Mangel an Transparenz und undemokratisch bemängeln. Auf Bedenken stößt besonders, dass Lobbyisten, etwa aus der Musik- und Softwareindustrie, bereits in die Ausarbeitung des Übereinkommens eingebunden sind.

Eckpfeiler des Übereinkommens soll eine verstärkte internationale Zusammenarbeit beim Bekämpfen der Produktpiraterie sein. Gegenstand der Verhandlungen soll auch die Art der Zusammenarbeit zwischen Internetprovidern und geschädigten Unternehmen sein. Auch für die Zollbehörden soll es weitreichende Befugnisse geben. Das bereits in den USA eingeführte Recht, Medienträger von Reisenden an Grenzen durchsuchen und einbehalten zu dürfen, soll ebenso eingeführt werden wie eine strafrechtliche Verfolgung von Urheberrechtsverstößen auch dann, wenn keine Bereicherungsabsicht vorliegt. *Tobias Haar*

Watchblogs dürfen fremde Namen tragen

Wer eine .com-Webseite in böser Absicht registriert, an der registrierten Domain keine Namensrechte hat und Dritte über die Herkunft der Domain täuscht, den kann die World Intellectual Property Organisation (WIPO) auf Antrag eines Namensrechtsinhabers zur Löschung der Domain zwingen. Jetzt ist eine solche Beschwerde gegen den Inhaber eines Watchblogs aber gescheitert. Geklagt hatte der Finanzdienstleister MLP gegen die Nutzung von „MLPwatchblog.com“ für eine Webseite. Die WIPO-Richter waren der Meinung, dass den deutschen Internetnutzern klar sein müsse, dass sich hinter dem Begriff „watchblog“ gar nicht der Finanzdienstleister selbst verbergen muss. *Tobias Haar*

Creative-Commons-Lizenzen 3.0 auf Deutsch

Nach der Anpassung an internationale Lizenzen und deutsche Urheberrechtsreformen ist kürzlich Version 3.0 der Creative-Commons-Lizenzen auf Deutsch erschienen. Diese Standardlizenzen beschreiben aus dem Open-Source-Gedanken abgeleitete Lizenzierungsmodelle für kreative Inhalte. Geschützte Werke stehen, wenn sie unter einer Creative-Common-Lizenz stehen, Dritten zur Nutzung zur Verfügung. Der Nutzer muss also nicht bei jeder einzelnen Verwendung beim Urheber um Erlaubnis nachfragen, solange er sich im Rahmen der Lizenz bewegt. Die Lizenz gestattet nun – entsprechend den Gesetzesänderungen – Nutzungsrechte auch für künftige, bei Lizenzeinräumung noch unbekannte Nutzungsarten. Andere Änderungen betreffen den Umgang mit gesetzlichen Vergütungsansprüchen. *Tobias Haar*

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Suns Fire X4450 auf 24 Cores ausgebaut

24 Prozessorkerne haben die x64-Server Sun Fire X4450 und Sun Blade X6450 nun zu bieten. Die mit vier CPU-Sockeln bestückten Rechner hat Sun mit Intels Xeon X7460 (Codename Dunington) ins Programm aufgenommen. Der 2,66 GHz schnelle Prozessor mit seinen sechs Kernen besitzt einen 16 MByte großen Level-3-Cache.

Suns X4450 kam mit dem neuen Xeon beim SAP SD in die Ränge und hält derzeit Platz zwei hinter HPs ProLiant DL580 G5. In den SPEC-Charts liegt sie im CINT2006 bei 22,0 (25,3), im CFP2006 bei 22,3 (23,6) und schafft bei den Rates 266 (289) beziehungsweise 141 (150). Die Blade X6450, mit vier E7450 ausgestattet, hat sich im CPU2006 mit 225 (241) CINT2006 Rates und 117 (128) CFP2006 Rates hinter Dell und HP eingereiht (Peak in Klammern). Die Benchmarks kamen unter SLES10 mit Intels Compilern in der Version 11 zustande.



Aufgemotzt: Suns Fire X4450 mit Intels Sechs-Kernern bestückt läuft mit 24 CPU-Cores und ist für Windows, Linux und Solaris zertifiziert.

Für die x64-Server bietet Sun als Betriebssystem Linux, Windows Server und das hauseigene Solaris 10 an. Der Preis für eine X4450 mit vier X7460-CPUs (2,66 GHz), 24 GByte Hauptspeicher und vier 146 GByte großen SAS-Platten liegt bei 18 900 €, der für eine X6450-Blade mit denselben CPUs, aber nur 16 GByte RAM, bei 15500 €.

iX-Link ix0811022

Adobe räumt sein Suites auf

Zwar bleibt die Grundanordnung der sechs Suites bei Adobe nach der Integration der Makromedia-Produkte erhalten, aber im Einzelnen gibt es Veränderungen: In die Design Premium Suite ist Fireworks mit eingezogen, dafür setzte der Hersteller Golive zu Gunsten von Dreamweaver auf die Straße. Beim internen Datenaustausch sprechen die Anwendungen nun XFL, in dem Adobes Flash-Format (FLA) einkapselt ist.

Photoshop CS4 simuliert mit einer drehbaren Arbeitsfläche bei der Bildbearbeitung den Umgang mit herkömmlichem Papier und bietet ein Werkzeug zum Beschneiden von Bildern, das relevante Teile automatisch verschonen soll.

Die Version für 64-Bit-Windows-Vista kommt in dem Genuss von mehr Arbeitsspeicher; Macianer müssen auf die nächsten Photoshop-Version warten. „Preflight“ findet der Publisher auf seinem Desktop, es klopft mit der Indesign-Funktion bereits dem Layouter auf die Finger.

Alle CS4-Anwendungen laufen unter Mac OS X und Windows XP/Vista. Photoshop CS4 gibt es für 1011 Euro, die Design-Premium-Suite inklusive Photoshop Extended, Illustrator, Flash Professional, Dreamweaver, Fireworks (alle CS4) sowie Acrobat 9 Pro kostet 2617 Euro. Die Videoschnitt-Suite Production Premium mit neuen Versionen von AfterEffects, Premiere Pro, Illustrator, Flash Professional und Photoshop Extended, schlägt mit etwa 2500 Euro zu Buche, für die Master Collection mit allen CS4-Produkten nebst Acrobat 9 Pro muss man 3569 Euro auf den Tisch legen.


iX-Link ix0811022

Intel präsentiert neue Version von vPro

Das auf dem Q45 Chipsatz basierende vPro soll Rechner umfangreicher verwalten als die bisherige Version vPro 2.0. Neben PCs können Systemadmins Notebooks über das WLAN fernsteuern. Allerdings muss es an das Stromnetz angeschlossen sein. Mit dem „IT-Director“ kann der Admin Rechner anhand ihrer MAC-Adressen selbst außerhalb der Firewall identifizieren und verwalten. Die Basissoftware Active Management Technology liegt in der Version 5 vor. Über Sicherheitsroutinen kann der Admin vPro-Clients, die eine Bedrohung darstellen, automatisch isolieren. *Nikolai Zotow*

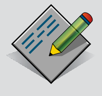
iX-Link ix0811022

Citrix’ XenServer hochverfügbar

Marathon Technologies’ Software Everrun ist fester Bestandteil der neuen Version des XenServers von Citrix mit Codenamen Orlando. Es gibt vier Stufen: HA für einfache Hochverfügbarkeit, FT für fehlertolerante Systeme, Splitside für große Entfernungen zwischen den HA-/FT-Servern und CDP & DP für Datensicherheit im WAN. Die letzten drei Optionen sind nach wie vor als Zusatzprodukt erhältlich. EverRun VM Lockstep Level Drei soll im ersten Quartal 2009 folgen und auf Betriebssystemebene Applikationen, die nicht ausfallen dürfen (Zero Downtime), vor Fehlfunktionen schützen.


iX-Link ix0811022

KURZ NOTIERT



Federwolken: Ein neues Betriebssystem mit dem vorläufigen Namen Windows Cloud hat Microsoft-CEO Steve Ballmer auf einer Partner-Veranstaltung in London angekündigt. Noch im Oktober will Microsoft es der Öffentlichkeit vorstellen.

Am Fenster: Amazon hat für sein Elastic Compute Cloud (EC2) die Unterstützung von Microsofts Server und SQL Server als Datenbank bekannt gegeben.

Rechenknechte: Microsofts Windows HPC Server 2008 (HPCS) heißt der Nachfolger des bisherigen Windows Computer Cluster Server 2003 (CCS). Als Grundlage dient Windows Server 2008 in der 64-Bit-Version. Wer sich bei Microsoft registriert, kann eine Version des HPCS 2008 zum Ausprobieren herunterladen.

Wahlweise: Kunden von Sun dürfen wählen, ob sie deren Virtual Desktop Connector oder VMwares Virtual Desktop Manager (VDM) mit der Virtual Desktop Infrastructure (VDI) einsetzen wollen. VMware hat Suns Ray Clients zertifiziert. Dazu soll es den kostenlosen Sun Ray Connector for VDM geben.

Dabeigeblieben: AMD kürt den Codename Fusion zum Markenzeichen des für 2009 geplanten Kombi-Chips, der Grafik- und Hauptprozessor vereint. Das umfasst auch das Konzept, die Prozessoren für andere Zwecke, etwa zum Number Crunching, zu nutzen.

Rechenexempel: Für 99 US-Dollar können Interessenten bei IBM ein Testdrive mit Microsofts Windows HPC Server 2008 mieten und aus der Ferne darauf zugreifen. Die Probefahrt findet auf 14 bis 16 Knoten in IBMs Bladecentern oder System-x-Servern auf Xeon-CPUs statt. Außerdem will IBM die 3D-Visualisierung Deep Computing Visualisation (DCV) für Nutzer des On-Demand-Angebotes bereitstellen.

Wolkenfrei: Oracle hat seine Datenbank 11g, Fusion Middleware und den Enterprise Manager für Amazons EC2 zertifiziert und liefert dazu frei erhältliche Amazon Machine Images (AMIs). Lizenzinhaber dürfen die zertifizierte Software ohne Zusatzkosten in EC2 verwenden. Darüber hinaus hat Oracle Secure Backup Cloud entwickelt, das aus den beiden Produkten Premier Tape Backup Management und Secure Backup von Oracle hervorgegangen ist.

Kleinzeichner: S3 Graphics bringt mit seinen Grafikprozessoren der Serie Chrome 400 ULP (Ultra Low Power) HD-Videos und DirectX-10.1-Spiele selbst auf die kleinsten mobilen Geräte und braucht dabei weniger als 7 W.

iX-Link ix0811022

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

VMware bringt Workstation 6.5

Zu den besonderen Neuerungen von VMwares Workstation 6.5 gehört Enhanced Execution Record/Replay. Das Werkzeug erlaubt es, das gesamte Systemverhalten inklusive CPU- und Geräteaktivität aufzuzeichnen sowie zu beliebigen Zeitpunkten Marker zu setzen.

Mit Unity können Anwender Fenster laufender Applikationen einer VM nutzen, als ob sie auf dem Host liefen. Anwendungen auf Windows-VMs können DirectX9 bis einschließlich Shader Model 2 benutzen. Virtual Machine Streaming verleiht Workstation 6.5 die Fähigkeit, VMs von einem Webserver schon während des Downloads laden und einschalten zu können. Mit Enhanced ACE Authoring (Assured Computing Environment) kann der Nutzer Sicherheitsoptionen wie Verschlüsselung, Gerätekontrolle und restriktiven Netzwerkzugang direkt aus der Applikation heraus konfigurieren. Damit erübrigt sich eine spezielle ACE-Edition.



Lenovo übernimmt ThinkServer

IBMs ThinkServer gibt es nun bei Lenovo mit Windows Server 2008 oder SLES 10. Der TS100 Tower und der RS110 fürs Rack sind mit Xeon- oder-Core-2-Duo-CPUs und 8 GByte Hauptspeicher bestückt, die beiden Tower-Modelle TD100 und TD100x sowie der Rack-Server RD120 arbeiten nur mit Xeons und können bis zu 48 GByte Hauptspeicher aufnehmen.

Zur Verwaltung sind dabei: ThinkServer EasyStartup zum Einrichten, ThinkServer EasyUpdate und ThinkServer EasyManage, das in Kooperation mit Landesk entstand. Erhältlich sind die Server ab 870 Euro für den TS100 (Xeon E3110, 3 GHz, 2 GByte RAM) und 3410 Euro für den RD120 mit zwei Quad-Core-Xeon Typ E5450 (3 GHz) und 4 GByte Hauptspeicher.



Statistiksoftware von SPSS in der Version 17.0 verfügbar

In der Version 17.0 seiner Software-Suite Statistics hat SSPS eine Reihe von Neuerungen eingebaut. Nicht nur bei der Darstellung von Tabellen und der grafischen Präsentation haben die Entwickler bei SPSS Hand angelegt, sondern vor allem bei den Analyse-Verfahren die Bedienung vereinfacht. Durch die Verbesserungen sollen selbst Anfänger mit der Software zurechtkommen. Experten hingegen dürften vom erweiterten Funktionsumfang profitieren.

Eine einfaches Drag & Drop erlaubt, es Darstellungen und Ergebnisse verständlich zu präsentieren, ohne dazu eine Programmiersprache nutzen zu müssen.

Die Integration der Predictive Enterprise Services und des Analytics Mining unterstützt vor allem die Bearbeitung von Daten im Unternehmen. Weitere Details sind unter www.spss.com/de/spss 17 zu finden.



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

DMS Expo: Zeit für das Wesentliche

Bodenständig

Achim Born

Konzentration auf das Kernthema, ein weitgehend traditionelles Rahmenprogramm – die diesjährige Messe und Konferenz für Enterprise-Content- und Dokumentenmanagement lief im gewohnten Trott. Das jedoch ist nicht zwangsläufig schlecht.

Wir bieten mit der DMS Expo eine zentrale Plattform für integrierte DMS, von der Erstellung über die Verteilung bis hin zur Ablage und Archivierung digitaler Dokumente." Der Satz im Abschluss-Statement von Oliver Kuhrt, Chef der Koelnmesse GmbH, beschreibt das Geschehen während der dreitägigen DMS Expo. Wer sich für die digitalisierte Informationsversorgung interessiert, kam am Besuch der Kölner Spezialmesse nicht vorbei, denn im Unterschied zu früheren Veranstaltungen waren die Anbieter von Enterprise-Content-Management- und Dokumentenmanagementsystemen (ECM/DMS) nahezu vollständig vertreten. Darunter sogar Google, Samsung und Oracle.

Wie in der Vergangenheit gab es ein breit gefächertes Rahmenprogramm, das alle Facetten der ECM/DMS einschließlich Langzeitarchivierung von PDF-Dokumenten (PDF/A) sowie digitaler Postbearbeitung bediente. Die Vorträge, Diskussionsrunden und Workshops trafen auf reges Interesse der Messebesucher, der zum Teil große Andrang belegte das überzeugend. Im Mittelpunkt der Vorträge standen in erster Linie pragmatische Aspekte. Vielfach leisteten die Redner Aufklärungsarbeit (etwa zur digitalen Steueraußenprüfung). Glaubt man einer Umfrage des VOI (Verband Organisations- und Informationssysteme), dem ideellen Träger der Messe, ist dies dringend geboten. Denn nach einer vom Verband im vergangenen Jahr durchgeführten Untersuchung haben erst 25 % der Unternehmen die Bedeutung und den Nutzen eines DMS vor dem Hintergrund gesetzlicher Regularien wie GoBS (Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme) oder GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen) erkannt.

Compliance liegt im Trend

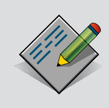
Die richtlinien- und gesetzeskonforme Dokumentenverwaltung, kurz Compliance, drängte sich auf vielen Ständen in den Vordergrund. Ein anderes auffälliges Thema: MOSS (Microsoft Office Sharepoint Server) – oder präziser die Kooperation mit dem Produkt. Beispielsweise vervollständigen Hersteller wie D.velop oder ELO ihre MOSS-Offerten um eine zentrale Ablage- und Archivierungskomponente. Microsoft selbst stellte den Office Sharepoint Server 2007 als zertifizierte Lösung vor, die dem hiesigen Handels- und Steuerrecht entspricht. In einer Beispielkonfiguration komplettierten das M-Archive for Sharepoint 2007 von Merentis und Netapps Speichersystem FAS270 den Server.

Ansonsten gab es kaum Veränderung zum Vorjahr, sieht man von produktbezogenen Neuerungen einmal ab. Anscheinend hat die Messe den Schwung, den sie im letzten Jahr aufgrund des Wechsels an den Rhein ausstrahlte, ein wenig eingebüßt. Mit rund 19 200 Fachbesuchern sowie 362 Ausstellern aus dreizehn Ländern konnte man nicht ganz das Vorjahresergebnis erreichen. (jd)

Content-Management als Service

Hyperwave präsentierte mit der Appswave-Linie eine gehostete Mietsoftware. Verfügbar ist ein Konferenzsystem, das Instant Messaging und Ad-hoc-Meetings inklusive VoIP- und Video-Funktion bietet. In Vorbereitung befindet sich eine Content-Management-Software, mit der Anwender ohne HTML-Kenntnisse Webseiten erstellen können sollen. Voraussichtlich zum Jahresende will man zudem mit Insync ein Programm für die zentrale Dokumenten- und E-Mail-Archivierung veröffentlichen.

KURZ NOTIERT



Alternative: CMS-Anbieter Alfresco zeigte eine Implementierung der Sharepoint-Services, über die Anwender von Microsofts Office-Produkten auf das Repository des Open-Source-CMS zugreifen können. Möglich ist dies, weil Microsoft die entsprechenden Protokolle auf richterlichem Druck offenlegen musste.

Personalverwaltung: Open Text führte die Version 2.0 von Employee Information Management vor. Dahinter verbirgt sich eine elektronische Variante der Personalakte, die speziell für das bidirektionale Zusammenspiel mit SAP HCM (Human Capital Management) konzipiert wurde. Neu in der Version 2.0 ist die Unterstützung von SAP ESS (Employee Self Service) und MSS (Manager Self Service).

Zusammengelegt: ASG Software, Spezialist für Archivierung und Records-Management, und Hitachi Data Systems verkündeten ihre Zusammenarbeit. Die gemeinsame Lösung bündelt die Archivierungssoftware ASG-Viewdirect mit dem Speichersystem Hitachi Content Archive.

Multilingual: Across Systems und Straker Interactive führten ein gemeinsames Produkt zum Webseiten-Erstellen und -Übersetzen vor. Beim Neubau einer Webseite schickt ShadoCMS von Straker die Inhalte automatisch zum Across Language Server. Der übersetzt den Input und übergibt ihn anschließend wieder an das Content-Management-System.

Trittbrettfahrer: Selbst war SER nicht vor Ort, stellte aber pünktlich zur DMS Expo seine Produktsuite Doxis4 vor. Das Dokumentenmanagementsystem enthält nun alles, was marketingmäßig en vogue ist: eine J2EE-basierte serviceorientierte Architektur mit Content Service Bus, Integrationsfähigkeit mit Drittsystemen durch Webservice-Interfaces sowie Rich Clients für Windows und Web.

Dezentral-zentral: NSi zeigte seinen Quickcapture Scan-Client, mit dem sich Desktop- oder Produktionsscanner in DMS-Lösungen integrieren lassen. Den Client kann man sowohl in zentralen als auch in dezentralen Scan-Szenarien einsetzen.

Leistungsshow: IBM-Tochter Cognos hatte die Version 9.4 von TM1 im Gepäck. Die Performance- und Controlling-Managementsoftware, die auf einem In-Memory-OLAP-Server (Online-Analytical-Processing) basiert, analysiert Geschäftsdaten in großen Volumina. In der neuen Version hat Cognos die Vorlagenerstellung, etwa für Reports, erheblich vereinfacht und die Integrationsfähigkeit mit Excel ausgebaut.

Geschäft messen: IDS Scheer bringt die Release 4.1.2 des Aris Process Performance Manager (PPM) heraus. Durch die Integration der Minitab-Statistik-Software lässt sich das Tool zum Messen von prozessorientierten Kennzahlen sowie im Controlling auch in Six-Sigma-Projekten nutzen. Darüber hinaus steht mit dem Query Web Service eine Schnittstelle zur Verfügung, die Daten online aus ARIS PPM extrahiert und in andere Applikationen einbettet.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Semiramis auf Nachfrage

Schon der frühere Eigner deutete wiederholt eine künftige On-Demand-Version der Unternehmenssoftware Semiramis an. Installiert im IBM Rechenzentrum, bietet SoftM die in Java programmierte ERP-Software nun als Service über das Internet an. Semiramis On Demand geht ab 6. Oktober in den Vertrieb, den Echtbetrieb will man im Folgemonat aufnehmen. Die Vermarktung übernehmen exklusiv die Semiramis-Partner, die auch Customizing-Dienstleistungen liefern. Preis pro Nutzer und Monat: ab 113 Euro.

Compliance mit Fabasoft

Die Enterprise-Content-Management-Software (ECM) Fabasoft Folio 2007 des gleichnamigen Linzer Softwarehauses stellt Dokumente und Daten in einem geschäftsbezogenen Kontext dar. So soll der Nutzer jederzeit Informationen zum Status der Geschäftsprozesse erhalten, etwa in Bezug auf rechtliche Anforderungen. Die Bedienoberfläche des neuen Folio steht als Browser-Variante und als Windows-Client zur Verfügung. Serverseitig arbeitet das Produkt mit Windows oder Linux. Als Datenbanksystem erwartet die ECM-Software einen SQL Server, Oracle oder PostgreSQL in der Fabalabs Edition.

Transparenz in die Geschäftsprozesse

Mit M3O Operations Book komplettiert Vitria seine gleichnamige Suite. Das Modul verknüpft Funktionen aus Business Intelligence (BI), Business Activity Monitoring (BAM) und Complex Event Processing (CEP) in einer Lösung. Anwender in den Fachabteilungen sollen darüber eine Vorstellung über die Qualität laufender Geschäftsprozesse erhalten. Dies ermöglicht ihnen, bei Abweichungen von den Sollwerten unmittelbar einzugreifen. Hierzu stellt die Komponente umfangreiche analytische Funktionen bereit.

Werkzeug für elektronische Beweisführung

IBM stellte seinen eDiscovery Manager vor, ein Tool für die gerichtsverwertbare Auswertung von E-Mails. Jedes Unternehmen, das eine Geschäftstätigkeit in den USA ausübt, muss diese Anforderung für US-amerikanische Zivilprozesse (Federal Rules of Civil Procedure, FRCP) erfüllen. Die Dokumente liegen in DB2-Content-Manager- oder Filenet-P8-Archiven, die zuvor mit IBM Commonstore oder dem Filenet E-Mail Manager aus den Exchange- oder Domino-Mailsystemen erstellt wurden.

In Kürze will IBM dem eDiscovery Manager eine Analysekomponente zur Seite stellen, die E-Mails automatisch nach potenziell relevanten Sachverhalten durchforstet. Der Manager ist Nachfolger der E-Mail-Suche aus Commonstore für Lotus Domino und Exchange Server. Und hinter der Analysekomponente steckt eine Spezialvariante der Omnifind-Suchmaschine.



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Bitkom sieht zu wenig E-Government für Unternehmen

Öffentliche Verwaltungen bieten Unternehmen in Deutschland zu wenig digitale Zugänge an, wie Bitkom in einer Studie feststellt. Demnach haben im Jahr 2007 nur 56 Prozent der Unternehmen hierzulande solche Behördenangebote genutzt – das bedeutet Platz 21 im Vergleich aller 27 Länder der europäischen Union. Den Spitzenplatz belegt Finnland (90 %), gefolgt von Irland (89 %), Dänemark (88 %), Luxemburg und der Slowakei (je 85 %).

Als Ursache kritisiert der Branchenverband eine fehlende Durchgängigkeit der ohnehin zu wenigen Angebote. Es müsse den Unternehmen leichter gemacht werden, mit Behörden digital zu kommunizieren, lautet die Forderung.

Außerdem erinnere die Realisierung der EU-Dienstleistungsrichtlinie (EU-DLR) derzeit an Kleinstaaterei. So sind die Planungen der Bundesländer derzeit unterschiedlich, an welcher Stelle der geforderte einheitliche Ansprechpartner anzusiedeln ist: bei den Kommunen, auf Kreisebene, bei den Kammern oder einer neu zu schaffenden Anstalt öffentlichen Rechts.

Der einheitliche Ansprechpartner soll die Anliegen von Unternehmen und Privatpersonen über Verwaltungs- und Zuständigkeitsgrenzen hinweg erledigen. Wie die neu einzuführenden Geschäftsprozesse zu modellieren sind, hat das Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin kürzlich in einem Bericht mit Empfehlungen für die IT-Umsetzung der EU-DLR vorgelegt. Die Ergebnisse des Forschungsprojekts „Prozessblaupause für die IT-Umsetzung der EU-Dienstleistungsrichtlinie“ stehen zum Download zur Verfügung auf www.prozessbibliothek.de.

Barbara Lange

Reputation von Mail-Versendern zentral eingeschätzt

Der Verband der deutschen Internetwirtschaft eco und Bizanga haben ein Abkommen geschlossen, in dessen Rahmen die vom eco verwaltete Absender-Whitelist Certified Senders Alliance (CSA) Eingang in Bizangas Reputationsdatenbank findet. Sie sammelt laufend Informationen über IP-Adressen und Domains von Mail-Absendern und dient dem schnellen Austausch dieser Informationen zwischen Providern für gemeinsame Abwehrmaßnahmen. Die Aufnahme der CSA-Positivliste soll Fehleinschätzungen von seriösen Werbemails als Spam reduzieren.

Die Datenbankserver sollen direkt im vom eco betriebenen zentralen Internet-Verkehrsknotenpunkt DE-CIX in Frankfurt unterkommen. Für neue Teilnehmer des Systems bietet Bizanga ein „Schnellstarterpaket“ an. Benutzer der Datenbank können Daten über ihre eigenen Verbindungen eingeben und die zur gemeinsamen Verfügung bereitgestellten Daten anderer Benutzer abfragen. Da Spammer häufig Mailhosts und verseuchte PCs in vielen Netzen zugleich nutzen, verspricht das gemeinsame Vorgehen eine schnellere Spam-Erkennung und -Abwehr.

Anzeige

E-Mail-Filterung als Managed Service für Großabnehmer

Eleven aus Berlin hat eine neue Version seines E-Mail-Filterdienstes eXpurgate vorgestellt. Mit einer um den Faktor 10 auf über 1000 E-Mails pro Sekunde gesteigerten Filterkapazität richtet sich die Version 3.0 laut Eleven an Carrier, öffentliche Einrichtungen und „Unternehmen jeder Größe“.

Zu den weiteren Neuerungen gehört die Unterstützung von Bounce Address Tag Validation (BATV) zum Schutz vor unerwünschten Rückläufern von Spam-Mails, deren Zahl in jüngster Zeit drastisch gestiegen ist.

eXpurgate 3.0 gibt es wahlweise als „Managed Service“ oder als Software. Beim Managed Service filtern Eleven-Server die E-Mails und leiten nur die als erwünscht klassifizierten an den Kunden weiter. eXpurgate steht auch als SDK für die Einbindung des Filters in Produkte und Anwendungen des Kunden zur Verfügung. Die Erkennungsrate des Filters beziffert Eleven auf über 99 Prozent.

Grün und konvergenzorientiert: Systems 2008

Am 21. Oktober eröffnet die Münchner Systems für vier Tage ihre Pforten, die zweitgrößte deutsche IT-Messse, die sich im Untertitel als „Entscheidermesse für IT, Media und Communications“ beschreibt. Nüchterner ausgedrückt geht es um eine B2B-Messe mit regionalem Schwerpunkt, die zwar in den letzten Jahren unter stetigem Schwund litt, aber 2007 immerhin noch mehr als 40 000 Besucher verzeichnete. Dieses Jahr verteilt sich die Ausstellung auf fünf Hallen: In den Hallen A1 und A2 geht es um „Software Solutions“, in B1 ist der Bereich „Communications & Networking“ zu finden, Halle B2 ist mit „Systems Integrations & Services“ überschrieben. Die zum zehnten Mal stattfindende IT-Security-Area schließlich bestimmt das Geschehen in Halle B3. Neue Schwerpunkte in München sind Green IT und Unified Communications, was sich auch in auf diese Themen ausgerichteten Sonderveranstaltungen ausdrückt.

Weitere Informationen und Onlineanmeldung: www.systems.de



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Schwachstellen in Datenbanken finden

Nach Sicherheitslücken speziell in Datenbanken sucht die neue Vulnerability-Appliance FortiDB-1000B, die der Hersteller Fortinet als die erste einer Serie vorstellt. Dazu zählen etwa Schwachstellen in Passwörtern, Zugriffsberechtigungen und Konfigurationen von Datenbanken. Auch warnt die Appliance Systemadministratoren vor potenziellen Bedrohungen und gibt Hinweise zur Erfüllung regulatorischer oder branchenspezifischer Pflichten – Stichwort „Compliance“. Sie ist einsetzbar in heterogenen Umgebungen mit Oracle, DB2, Sybase und SQL. FortiDB-1000B kann bis zu 30 Datenbanken gleichzeitig handhaben, die nächsten beiden Versionen sollen 10 beziehungsweise 60 Datenbankinstanzen managen. Eine Softwareversion für große Unternehmen mit mehreren Tausend Datenbanken ist bereits verfügbar.

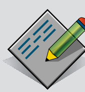


Zutrittskontrolle und Zeiterfassung per Handy

Sorex Wireless stellt zur Sicherheitsmesse „Security Essen“ das System „Wireless Key“ vor, das Bluetooth-fähige Handys in Türschlüssel verwandelt (www.sorex-austria.com). Das System besteht aus einem 12 × 12 Zentimeter großen Hardwaremodul für die Montage auf der Innenseite einer Tür. Administratoren können die über IP erreichbaren Module zentral verwalten und pro Tür bis zu 2500 Handys registrieren. Am Mobiltelefon selbst sind keine Veränderungen erforderlich. Nach Angaben des Herstellers wird nur bei der ersten Anmeldung ein 128-Bit-verschlüsselter Autorisierungscode ausgetauscht. Die Tür öffnet sich, wenn sich das Handy nähert. Einstellbar sind Distanzen von wenigen Zentimetern bis 14 Metern.

Barbara Lange

KURZ NOTIERT



Verschlüsselung I: PGP veröffentlicht sein Produkt PGP Command Line in einer nativen Version für Mainframes der IBM zSeries. Damit können Systemverantwortliche vertrauliche Daten direkt auf Großrechnern mit dem Betriebssystem z/OS verschlüsseln, ohne sie vorher auf ein anderes System transferieren zu müssen.

Verschlüsselung II: UM Labs (www.um-labs.com), Anbieter von Sicherheitsprodukten für Unified Messaging und VoIP, hat Phil Zimmermanns ZRTP in seine Produkte integriert. ZRTP ist eine Erweiterung des Datenübertragungsprotokolls RTP, es verschlüsselt Sprach- sowie Videoströme. Das Besondere ist laut Hersteller der sichere Schlüsselaustausch über den Sprachkanal, sodass er im Gegensatz zu dem üblicherweise über den Signalisierungskanal versendeten Schlüssel nicht sichtbar und für einen „Man in the Middle“ nicht abzufangen ist.

Sandkiste für Pinguine: Norman (www.norman.com/de), „Erfinder“ der isolierten Umgebung für Malware-Analyse, stellt seine Sandbox-Produktreihe in neuer Version vor. Die Produktreihe läuft nun auch auf Linux-Rechnern. Neben ausführbarem Code analysieren die Produkte überdies Exploits in Microsoft Office und weiteren gängigen Programmen, ein neuer Emulator soll zudem den Analyseprozess beschleunigen und die Erkennungsrate um 20 % steigern.

iX-Security-Special mit Multiboot-DVD

Gleichzeitig mit dieser Ausgabe erscheint das *iX* Special „Sicher im Netz“ . Auf über 150 Seiten geht es um die Security-Probleme, die heute Administratoren, Beratern und Sicherheitsbeauftragten auf den Nägeln brennen – von Websicherheit über externe und interne Angriffe, Werkzeuge zur Einbruchserkennung bis zu rechtlichen und Management-Fragen.



Dem Heft liegt eine Multiboot-DVD bei, die eine Systemuntersuchung oder -reparatur ohne Software-Installation erlaubt. Bei den bootbaren Systemen handelt es sich um das Avira Rescue System, Backtrack 3, Damn Vulnerable Linux, DAVIX und Recovery Is Possible. Außerdem befinden sich auf der DVD Security-Tutorials sowie über 50 Tools – Forensik-Werkzeuge, Rootkit-Entferner, Virenscanner und so weiter.

Das *iX* Special ist im gut sortierten Zeitschriftenhandel sowie online erhältlich (www.heise.de/kiosk/special/).

Zertifizierung für Softwaresicherheit

(ISC)2 (ISC-squared), die gemeinnützige Organisation zur berufsbegleitenden Ausbildung und Zertifizierung von IT-Sicherheitsexperten, plant eine Zertifizierung im Bereich Softwaresicherheit einzuführen. Der Certified Secure Software Lifecycle Professional (CSSLP) soll die Zahl von Sicherheitsschwachstellen in der Software reduzieren. Behandelte Themen sind Softwarelebenszyklus, Schwachstellen, Risiken, Grundlagen der Informationssicherheit und Compliance.

Die codeneutrale Zertifizierung ist für alle am Softwarelebenszyklus beteiligten Berufsgruppen relevant, etwa für Prozessanalysten, Entwickler, Softwareingenieure, Softwarearchitekten, Projektmanager, Softwaretester und Programmierer.

Die erste Prüfung soll Ende Juni 2009 stattfinden. Deshalb sucht (ISC)2 qualifizierte Softwarespezialisten, die sich an der abschließenden Entwicklung des Zertifizierungsverfahrens beteiligen wollen.

Susanne Franke

Websense mit Content-Erkennung

Websense hat seine Web Security Version 7 vorgestellt. In der jüngsten Release ist ein neues optionales Content-Gateway-Modul hinzugekommen. Es handelt sich dabei um einen Web-Proxy, mit dem Anwender auch verschlüsselten Datenverkehr analysieren oder eine Web-2.0-Kategorisierung vornehmen können, weil sich der Datenstrom intensiver analysieren lässt. URLs werden auch dynamisch klassifiziert. Das heißt, den Verkehr müssen nicht mehr die Websense Security Labs kategorisieren, dies erfolgt am Gateway. Außerdem ersetzt eine Weboberfläche das bisherige Java-Interface. Neu ist auch die Integration von Verwaltungs- und Reporting-Tools auf einer einheitlichen Benutzeroberfläche. Ein Management-Dashboard zeigt alle Security-Vorfälle. Das ebenfalls neue Modul „Data Security Endpoint“ schützt gespeicherte Daten (Data at Rest), bearbeitete Daten (Data in Use) und gerade übertragene Daten (Data in Motion). Die Software verhindert das unerlaubte Kopieren vertraulicher Unternehmensdaten auf USB-Sticks.

Susanne Franke

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Hitachi Data Systems erweitert AMS-Familie

Um die Lücke zwischen Midrange- und Highend-Storage zu schließen, ergänzt Hitachi Data Storage (www.hds.com) seine AMS-Speicherfamilie (Adaptable Modular Storage) um die AMS2000-Serie. Sie besteht zunächst aus den Modellen AMS2100, 2300 und 2500.

Intern setzen die Geräte auf die moderne SAS-Technik (Serial Attached SCSI). Sie erlaubt es, sowohl SAS- als auch SATA-Festplatten einzusetzen. Zur Wahl stehen 3,5" große SAS-Modelle mit 146 und 300 GByte Kapazität bei 15 000 U/min oder 400 GByte bei 10 000 U/min sowie SATA-Festplatten mit einer Drehzahl von 7200 U/min und 500, 750 oder 1000 GByte. Mischbestückung ist möglich, sofern jede RAID-Gruppe aus Platten einer Bauart besteht. Zwischen SAS- und SATA-RAIDs lassen sich Daten automatisch migrieren. Wer angesichts des Vollausbaus mit 120, 240 respektive 480 Platten Strom sparen will, kann ungenutzte RAID-Gruppen herunterfahren (Spin-down).

Alle Modelle besitzen zwei Controller, die im active/active-Betrieb arbeiten (Load Balancing) und die RAID-Level 0, 1, 5, 6 und 10 beherrschen. Aus Sicherheitsgründen verweigern die Controller den Betrieb von SATA-Platten als RAID 0 – der Hersteller empfiehlt, RAID 6 zu verwenden.

Das Modell 2100 bietet 4 bis 8 GByte Cache pro Controller und insgesamt vier Host-Ports – wahlweise 4 GBit/s FC oder 1 GBit/s Ethernet (iSCSI). Die größeren Exemplare AMS2300 und 2500 stellen die doppelte und vierfache Menge an Ports und Cache zur Verfügung. AMS2100 und 2300 sind bereits verfügbar, das Modell 2500 soll im ersten Quartal 2009 erhältlich sein.

iX-Link ix0811030

IT-Equipment auf der Schiene

Fujitsu Siemens Computers hat die Beförderung von Monitoren und Barebone-Gehäusen von China nach Deutschland auf die Schiene verlagert. Als erster IT-Produzent nutzt FSC die neue transeurasische Strecke der DB Schenker mit sogenannten „Dedicated Company Trains“, die ausschließlich Fracht eines Herstellers befördern. Am 6. Oktober kam der erste Zug nach einer 17-tägigen Reise von Xiangtang, etwa 700 km nördlich von Hongkong, in Hamburg an. Erst im Januar dieses Jahres hatte der erste Testzug der DB Schenker seine 10 000 km lange Fahrt absolviert.

Dass FSC einen Teil seiner zeitkritischen Transporte von den Luftwegen auf die Schiene verlagert, begündet der Hersteller damit, dass sich dadurch der CO_2-Ausstoß auf 5 % und die Kosten auf ein Viertel reduzieren. Gegenüber der Seefracht beschleunigt sich der Transport um etwa zehn Tage.



Für die 10 000 km lange Strecke von Xiangtang nach Deutschland benötigt der Trans-Eurasia-Express 17 Tage. Zweimal muss er dabei wegen des Wechsels der Spurbreite Lok und Waggons austauschen.

AMD stellt neue Profi-Grafikkarten vor

Einen Monat nach der Einführung der Firepro-Grafikkarten-Familie für CAD- und DCC-Anwender (Digital Content Creation) hat AMD zwei weitere Modelle, Firepro V8700 und V3750, vorgestellt. Im Unterschied zu den Karten der nun abgelösten FireGL-Serie bieten die V8700 und V3750 einen Dual-Link-DVI- und zwei Displayport-Ausgänge.

Wie die auf der Siggraph 2008 vorgestellten Brüder Firepro V5700 und V3700 unterstützen die Neulinge Microsoft DirectX 10.1, OpenGL 2.1 mit OpenGL Shading Language sowie das Shader Model 4.1 und kommunizieren über ein PCIe-2.0-x16-Interface. 800 Shader-ALUs (Arithmetic Logic Units), RV770-Grafikchip und 1 GByte GDDR5-Speicher mit einem Durchsatz von 108,8 GByte/s zeichnen das neue Highend-Modell V8700 der Profi-Serie aus, während sich die Firepro V3750 mit 320 Shader-ALUs, RV730-Grafikchip und 256 MByte 22,4 GByte/s schnellem GDDR3-Speicher direkt neben der V5700 ansiedelt.

Die Auslieferung der Firepro V8700 und V3750 soll im vierten Quartal 2008 beginnen. AMD empfiehlt einen Einzelhandelspreis von 1499 respektive 199 US-Dollar. Bereits jetzt sollen die Modelle Firepro V5700 und V3700 für 599 beziehungsweise 99 US-Dollar verfügbar sein.

iX-Link ix0811030

256-GByte-SSD von Toshiba

Auf der japanischen Elektronikmesse CEATEC 2008 hat Toshiba seine neue 2,5"-SSD (Solid State Disk) THNS256G E8BC mit SATA-II-Schnittstelle vorgestellt. Der Hersteller verspricht eine Schreibgeschwindigkeit von 70 MByte/s und eine Lesegeschwindigkeit von 120 MByte/s. In einem 2,5"-Gehäuse arbeiten NAND-Flash-Module mit der Größe von 70,6 mm × 53,6 mm und einer Höhe von 3 mm. Mit dieser Technik ist es recht einfach, höhere Speicherkapazitäten zu erreichen. So kündigte Toshiba eine 512-GByte-SSD bereits für 2009 an. Die Serienfertigung der 256-GByte-SSD soll noch im vierten Quartal 2008 beginnen, den Preis hat Toshiba aber noch nicht bekanntgegeben.

Ebenfalls im September hat Toshiba eine 1,8"-Festplatte mit 250 GByte vorgestellt. Für die MK2529GSG hat der Hersteller die Speicherdichte auf 378,8 GBit/in^2 erhöht. Ausgestattet ist sie mit zwei Scheiben und 1,5-GBit/s-Mini-SATA-Schnittstelle.

Axel Urbanski

iX-Link ix0811030

Festplatten-Verschlüsselung per Hardware

Meist ist menschliches Versagen die Ursache, wenn vertrauliche Daten aus Unternehmen „entweichen“ – etwa wenn eine Firma alte Festplatten ausmustert, ohne sie vorher zu löschen. Dem lässt sich nur durch konsequentes Verschlüsseln aller Daten vorbeugen.

Für seine System-x-Servermodelle x3650, x3655, x3550, x3500, x3400, x3350 und x3250M2 bietet IBM den SAS/SATA-RAID-Controller ServeRAID-MR10is VAULT mit integrierter Hardware-Krypto-Engine an. Die PCI-Express-Steckkarte (8x) beherbergt den RAID on Chip (ROC) LSISAS1078DE von LSI sowie 256 MByte Cache. Eine Pufferbatterie erhält die Daten auch bei einem Stromausfall von maximal 72 Stunden. Der Controller kann acht Platten bedienen und beherrscht die RAID-Level 0, 1, 5, 6, 10, 50 und 60. Zur Verschlüsselung benutzt er den Standard IEEE 1619 XTS-AES 256.

Auf der Liste der unterstützten Betriebssysteme stehen neben Windows auch Red Hat, Suse Linux und VMware. IBM nennt für den ServeRAID MR10is VAULT einen Listenpreis von 875 Euro.

iX-Link ix0811030

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Mono-Version 2.0 freigegeben

Die Entwickler von Mono, der Open-Source-Alternative zu .Net, haben die Version 2.0 fertiggestellt. Laut Release-Notes (www.mono-project.com) bietet die aktuelle Ausgabe fast den gleichen Funktionsumfang wie Microsofts Original, das .Net-Framework 2.0. Neben einigen spezifischen Eigenschaften, wie der Gtk#-API, unterstützt Mono unter anderem Windows.Forms (Desktop-Anwendungen), ADO.Net (Datenbankzugriff) , ASP.Net (Web-Anwendungen) und System. Drawing (portable Grafikausgaben). Monos C#-Compiler beherrscht den kompletten Sprachumfang von C# 3.0 inklusive der Datenabfragesprache LINQ. Darüber hinaus gehört ein Compiler für Visual Basic 8.0 zum Lieferumfang.



Open-Source-Texterkennung

Die Schweizer Firma Archivista hat sich auf Dokumenten-Management-System-(DMS)-Appliances spezialisiert. Die jetzt vorgestellte Version 2008/IX der DMS-Appliance ArchivistaBox enthält die laut Hersteller weltweit erste Open-Source-Texterkennung, die den erkannten Text in indexierten, durchsuchbaren PDF-Dateien ablegen kann. Das auf Sourceforge gepflegte freie DMS soll rund 20 verschiedene Sprachen erkennen und steht unter der GPLv2.

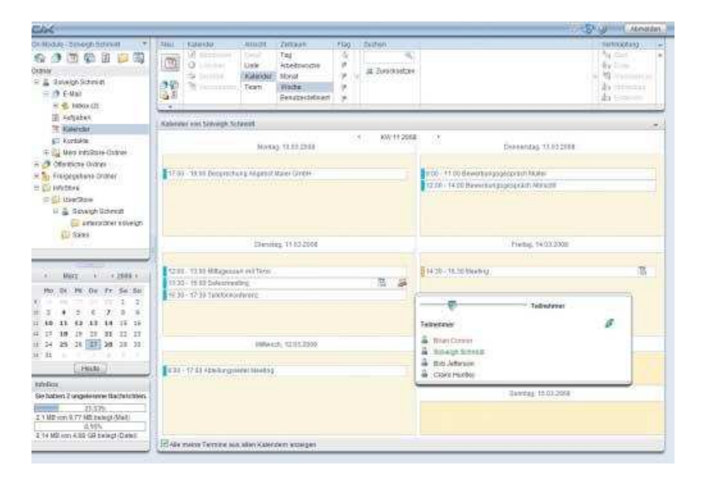


Groupware aktualisiert

Open-Xchange (OX, www.open-xchange.com/de) hat seine gleichnamige Linux-Groupware aufpoliert. Zunächst aktualisierte man die für ISPs gedachte Hosting Edition, jetzt folgte die für den Einsatz im Unternehmen konzipierte Server Edition. Damit verwenden beide Varianten der seit Februar fast vollständig unter der GPL stehenden Software die gleiche Codebasis in der Version 6. Sie bieten unter anderem ein Ajax-GUI, das sich über Themes und Skins an das jeweilige Firmendesign anpassen lässt. Funktionale Erweiterungen kann man entweder als Plug-ins direkt in die Oberfläche oder über das Universal Widget API (UWA, dev.netvibes.com/doc/universal_widget_api) in die Startseite integrieren.

Mit Debian Etch, RHEL 5 oder SLES 10 unterstützt die OX Server Edition die im professionellen Umfeld gängigsten Linux-Derivate. Sie lässt sich gut in bestehende LDAP- oder Active-Directory-Umgebungen integrieren. Der Vertrieb soll weitgehend über Partner erfolgen. Eine Software-Subskription inklusive aller Bugfixes und Updates für ein Jahr kostet für 25 Anwender 875 Euro/218,75 Euro (1. Jahr/Folgejahre). Kunden mit laufender Subskription können jederzeit kostenlos auf die neue Version wechseln.





Weiße Flecken auf der OSS-Karte

Mit ihrer Liste von elf „High Priority Free Software Projects“ (siehe Kasten) will die Free Software Foundation (FSF) etwas gegen ihrer Meinung nach zu wenig erschlossene Gebiete auf der virtuellen Free-Software-Landkarte unternehmen und so die Akzeptanz freier Programme steigern. Zu der unter www.fsf.org/campaigns/priority.html veröffentlichten Liste der als besonders wichtig angesehenen, fehlenden Anwendungen finden sich Anregungen, wie sich auch Nicht-Entwickler an den jeweiligen, teils noch zu gründenden Projekten beteiligen können.



High Priority Free Software Projects

1. Gnash – freier Flash-Player
2. Coreboot – Open-Source-BIOS
3. freies Pendant zu Skype
4. kommunikative Mitglieder- und Spendeninfrastruktur
5. freie Videobearbeitungssoftware
6. freier Google-Earth-Ersatz
7. gNewSense – GNU/Linux-System ohne proprietäre oder lizenzrechtlich bedenkliche Komponenten
8. Octave – Matlab-Ersatz
9. freier Ersatz für OpenDWG-Bibliotheken (CAD)
10. GDB um „Reversible Debugging“ erweitern
11. freie Treiber für Router

Rente mit Linux berechnen

Zur Umsetzung von Sparvorgaben stellen vier deutsche Rentenversicherer Teile ihrer Anwendung von IBMs Mainframe-Betriebssystem z/OS auf Linux um. Hintergrund: Nach einem 2004 formulierten Ziel im Gesetz zur Organisationsreform der deutschen Rentenversicherung (RVOrgG) sollen die Träger ihre Verwaltungskosten um 350 Millionen Euro jährlich reduzieren. Einen Beitrag dazu sollen eingesparte Lizenzkosten für z/OS und IBMs Transaktionsmonitor CICS leisten.

Der neue Linux-Rechner läuft in einer Mainframe-Partition und betreibt das „Gemeinsame Rentenversicherungssystem“ der DRV-Versicherungsträger aus Baden-Württemberg, Hessen, dem Saarland sowie der Knappschaft-Bahn-See. Dazu verwendet er neben der Cobol-Implementierung von Microfocus Claritys Transaktionsmonitor Unikix TPE. Die Datenhaltung erfolgt weiterhin via DB2 unter z/OS.

iX-Link ix0811032

KURZ NOTIERT

Absolventenpreis: Univention lobt zum zweiten Mal den mit insgesamt 3000 Euro dotierten Absolventenpreis für herausragende Abschlussarbeiten mit einem Open-Source-Thema aus. Bewerber können ihre Arbeiten bis 19. April kommenden Jahres unter www.absolventenpreis.de einreichen, die Preisverleihung wird während des Linuxtags 2009 stattfinden.

Verspätung: Wegen eines Fehlers im Datenbankmodul Base haben die Openoffice-Entwickler das für Ende September vorgesehene Release-Datum der Version 3.0 verschoben. Wenn mit dem jetzigen Release Candidat 4 alles klappt, dürfte Openoffice 3.0 mit Erscheinen dieser Ausgabe zur Verfügung stehen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Standorte verbinden mit Dynamics AX

Microsoft hat seine ERP-Software Dynamics AX 2009 laut eigenen Aussagen mit rund 400 neuen Funktionen ausgestattet, beispielsweise in den Bereichen Supply Chain Management (SCM) und Human Resources (HR). Die neue Version wendet sich vor allem an Kunden, die mehrere Niederlassungen betreiben. Sie bietet über das Shared Service Center die Möglichkeit, dass beispielsweise Niederlassungen als zentrale Bearbeitungsstelle für andere Zweigstellen fungieren – etwa für den Zahlungs- und Rechnungsverkehr. Webservices erledigen den technischen Part der Anbindung. Hinzugekommen sind automatisierte Standardabläufe in Form von Workflows, die die Einhaltung rechtlicher Regelungen erleichtern sollen, sowie ein Compliance Center, das interne Kontrollmechanismen und Kennzahlen darstellt. Dynamics AX enthält entsprechende länderspezifische Funktionen für 36 Staaten. Schließlich verschafft das Role Center einen Überblick über die Tätigkeiten jedes Angestellten. Ab Dezember bietet Microsoft auch die kleinere Variante Dynamics NAV 2009 mit Role Center und erweiterten Reporting-Funktionen an.

Susanne Franke

Offener ECM-Standard geplant

Einige namhafte Anbieter (IBM, Microsoft, EMC, Alfresco, Opentext, Oracle, SAP) haben eine Schnittstellenspezifikation für Enterprise-Content-Managementsysteme (ECM) entwickelt. Die Beteiligten wollen die Spezifikation namens Content Management Interoperability Services (CMIS) von der Standardisierungsorganisation OASIS absegnen lassen. Der Anspruch ist groß: Wie SQL im Datenbankbereich soll CMIS die Zusammenarbeit zwischen proprietären ECM erlauben. Alfresco hat bereits die erste Implementierung zum Ausprobieren vorgestellt. CMIS ist noch weit von einem Standard entfernt. Wie sich die Spezifikation mit anderen Versuchen, die Ähnliches propagieren, namentlich WebDAV und JSR 170 (Content Repository for Java), verträgt, lässt sich noch nicht abschätzen. Mit der Java-Schnittstellenspezifikation JSR 170 harmoniert CMIS laut Aussagen aus dem ECM-Umfeld gut, die HTTP-Erweiterung WebDAV könnte Leidtragende des Standardisierungsversuchs werden.





Java-Tools: Oracle hat die Version 11g sowohl der Entwicklungsumgebung JDeveloper als auch des Application Development Framework (ADF) angekündigt. Beide Produkte gehören zu Oracles Fusion Middleware und bieten beispielsweise die Möglichkeit, Anwendungen gleichzeitig für Desktop- sowie mobile Anwendungen zu entwickeln.

Standardhilfe: JD Edwards Enterprise One liegt in Version 9.0 vor. Oracles zugekaufte ERP-Software enthält ein Projekt- und Abrechnungsmodul für Regierungsaufträge. Die Komponente soll Ingenieursfirmen den Umgang mit US-Standards wie Federal Acquisition Regulation (FAR) und U.S. Cost Accounting Standards (CAS) erleichtern.

Multitalent: Magic Software hat die Entwicklungsplattform uniPaaS als Nachfolger des eDeveloper freigegeben. Laut Magic können die Anwender wählen, in welchem Modus ihr Programm arbeiten soll. Zur Auswahl stehen: Full Client, Rich Client, Webanwendung, On-Demand, On-Premise und SaaS. In Rich Internet Applications (RIA) erledigt uniPaaS automatisch die Client-Server-Partitionierung.

iX-Link ix0811034

SAP erweitert Metadatenverwaltung

Business Objects, SAPs Geschäftsbereich für Datenanalyseprodukte, hat die Version 3.0 Metadata Management XI vorgestellt. Die Anwendung soll das unternehmensweite Datenmanagement (Data Governance) vereinfachen. Sämtliche Informationen liegen konsolidiert in einem Repository. Das in die Business-Intelligence-Plattform XI integrierte Werkzeug bietet außerdem ein sogenanntes Metapedia, ein enzyklopädisches Verzeichnis, das unterschiedliche Metainformationen mit betriebswirtschaftlichen Begriffen verknüpft.

Centrasite mit SOA-Zuschnitt

In Centrasite ActiveSOA führt die Software AG ihre bisherige Centrasite Enterprise Edition mit der Governance Edition (vormals Webmethods Infravio) für SOA-Governance und Lifecycle-Management zusammen. Das Produkt fußt auf einer Registry, die sowohl das UDDI-Protokoll (Universal Description, Discovery and Integration) als auch JAXR (Java API for XML Registries) unterstützt. In einer Verbundarchitektur sollen sich Governance-Prozesse und Policies inklusive Metadaten über unterschiedliche, auch externe Repositories und SOA-Installationen hinweg synchronisieren lassen. Das System kooperiert mit verschiedenen Webmethods-Werkzeugen (ESB, Insight, Mediator) und soll so die zentralisierte Kontrolle und Durchsetzung von Regeln in verteilten SOA-Umgebungen ermöglichen. Der Anwender kann in Echtzeit Änderungen an SOA-Komponenten wie Services, Policies, Prozessen und Regeln bewerten. Eine spezielle Metrik erlaubt ihm, das Design von Komponenten zu kontrollieren und zu modifizieren. Schließlich ist eine auf Ajax beruhende, rollenbasierte Benutzeroberfläche hinzugekommen. Die Software AG will ActiveSOA im 2. Quartal 2009 allgemein freigeben, bisher dürfen nur ausgewählte Kunden das Produkt ausprobieren. *Susanne Franke*

Microsoft und SWIFT kooperieren

Microsoft geht eine globale Partnerschaft mit SWIFT ein, einem Provider für Finanztransaktionen. Ziel ist die Entwicklung von Lösungen für die Finanzindustrie sowie die Integration der IP-basierten Messaging-Plattform Swiftnet. Auf dieser Basis sollen externe Partner Produkte für die Finanzwirtschaft erstellen. Der Biztalk Accelerator hält die notwendigen Protokolle und Adapter für die Kommunikation mit dem Transaktionsnetzwerk der SWIFT bereit. Das Produkt soll als fester Bestandteil in den Biztalk Server 2009 eingehen, den Microsoft in der ersten Hälfte des kommenden Jahres vorstellen will.

Echzeitanalysen von Intersystems

Intersystems hat eine Echtzeit-Business-Intelligence-Anwendung namens DeepSee vorgestellt. Sie soll die Sparte Auswertungssoftware aus ihrer traditionellen Nische der strategischen Planung herausholen und auf die täglichen Entscheidungsprozesse aller geschäftlichen Ebenen ausweiten. Laut Hersteller bildet DeepSee eine kostengünstige Alternative zu den klassischen BI-Produkten, denn riesige Data Warehouses sind nicht erforderlich und der Consulting- und Implementierungsaufwand hält sich angeblich in engen Grenzen. DeepSee arbeitet direkt auf den transaktionsverarbeitenden Anwendungen. Für Entwickler stehen vorbereitete Grafiken, Diagramme, Tabellen, Reports und Dashboards für den Einbau in andere Applikationen bereit. Die Software ist unter Windows, Linux, Mac, Unix und OpenVMS verfügbar.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Management-Schulterschluss

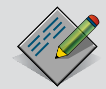
BMC und VMware wollen ihre Partnerschaft vertiefen. Hauptbestandteile der aktuellen Vereinbarung sind ein neuer Wiederverkäufervertrag und die gemeinsame Entwicklung eines integrierten IT-Managementsystems, das auf VMwares vCenter Lifecycle Manager und BMCs Remedy IT Service Management (ITSM) sowie BMCs Atrium Orchestrator (ehemals Run Book Automation) basieren wird.

Diese Produktkombination soll zu VMware-optimierten Automatisierungswerkzeugen mit einer einzigen Schnittstelle für Serviceanfragen führen. So lässt sich damit ein Change- und Konfigurationsmanagement über heterogene virtualisierte und nicht virtualisierte Rechenzentren realisieren. Zu kaufen gibt es die integrierte Lösung – und damit den VMware vCenter Lifecycle Manager – bei BMC.

i-doit nimmt Kontakt zu Nagios auf

Das i-doit-Projekt stellt für das gleichnamige Infrastruktur-Dokumentationswerkzeug eine Kopplung zur Netzüberwachungssoftware Nagios bereit. Administratoren können ihren Gerätepool auf diesem Weg einfacher steuern, da Überwachung und Dokumentation jetzt nicht mehr getrennt voneinander zu betrachten sind. Die unter www.i-doit.org frei beziehbare Schnittstelle liefert im ersten Schritt zwei Funktionen: Zum einen zeigt sie den von Nagios ermittelten aktuellen Status innerhalb der Objekte-Ansicht von i-doit in Ampelform an, zum anderen ermöglicht sie das Speichern von Statusmeldungen im betreffenden (i-doit)-Logbuch der Objekte, sobald Nagios Änderungsmeldungen generiert. Als nächster Schritt ist geplant, dass Anwender Objekte nicht nur dokumentieren, sondern auf Knopfdruck auch eine Nagios-Konfiguration erzeugen können. Das Open-Source-Tool i-doit geht auf eine Initiative des Düsseldorfer Infrastrukturspezialisten Synetics zurück.

KURZ NOTIERT



Schnell einführen: USU schnürt mit Valuemation Express ein Paket für die schnelle Umsetzung des IT-Asset-/IT-Service-Managements gemäß ITIL (IT Infrastructure Library). Vorkonfigurierte Vorlagen, Schnittstellen, Datenklassifikationen und Berechtigungen gewährleisten zusammen mit definierten Reports sowie Eskalationsregeln einen raschen Produktivstart. Das Paket umfasst ITIL-Prozessunterstützung, die Configuration Management Database (CMDB) sowie ein Kennzahlen-Cockpit.

Durchblick: Frontrange Visualization des gleichnamigen Anbieters bietet einen Überblick über die gesamte IT-Umgebung. Das Modul mit integrierter CMDB (Configuration Management Database) stellt die Beziehungen zwischen Unternehmens-Services und Konfigurationselementen der Infrastruktur grafisch dar. Auf diesem Weg lässt sich sofort erkennen, welche Auswirkungen Veränderungen in der IT-Infrastruktur auf die betrieblichen Abläufe haben.

Vor-Bildlich: Die Version 4.75 des Netzwerkscanners *nmap* erkennt nun iPhones, Systeme mit dem Linux-Kernel 2.6.25, Mac OS X, Darwin 9.2.2 oder Windows Vista mit Servicepack 1 anhand ihrer „Fingerabdrücke“. Die Zahl der Signaturen wuchs von 1320 auf 1503, während die Zahl der standardmäßig untersuchten Ports aus Performancegründen auf 1000 sank. Überarbeitungen erfuhr außerdem die grafische Oberfläche Zenmap. Dank der Integration des Visualisierungstools Radialnet lassen sich jetzt Karten der Netztopologie automatisch anlegen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Wunscharbeitgeber: Google jetzt vor SAP

Führungswechsel unter den Lieblingsarbeitgebern der Informatikstudenten in Deutschland: Der Suchmaschinenbetreiber Google läuft in diesem Jahr SAP den Rang ab. Das Walldorfer Softwarehaus, dem erst im vergangenen Jahr der Sprung an die Spitze gelang, muss heuer mit dem zweiten Platz vorliebnehmen. Allerdings konnte SAP schon 2007 Google mit einem Abstand von 0,1 Prozentpunkten nur knapp hinter sich lassen. In diesem Jahr erreichte die US-Firma einen deutlichen Vorsprung von 3,5 %. Mit diesem Wert ist sie das einzige Unternehmen, das gegenüber dem Vorjahr den Stimmenanteil nennenswert steigern konnte.

Google ist allerdings nicht für alle Teilgruppen der befragten IT-Studenten die Nummer 1. Technische Informatiker sowie Studierende der Wirtschaftsinformatik/Informationswirtschaft setzen das Unternehmen nur auf Platz 2. Stattdessen erkoren die Erstgenannten Siemens zur Nummer 1, die betriebswirtschaftlich angehauchten Informatiker setzten wiederum SAP an die Spitze. Gleiches gilt für die „High Potentials“ (Führungsnachwuchs für Managementaufgaben) unter den Informatikern, die ebenfalls SAP vor Google und der Unternehmensberatung Accenture zum beliebtesten Arbeitgeber wählten. Das sind Ergebnisse, zu denen das Berliner Trendence Institut in der zehnten Auflage seiner Studie „Das Deutsche Absolventenbarometer – IT Edition“ gelangte. In die diesjährige Untersuchung flossen Antworten von über 6300 Studenten an 63 deutschen Hochschulen ein.

Wunscharbeitgeber

Rang 2008	Unternehmen	Nennungen	Rang 2007	Nennungen
1	Google	19,5	2	16,2
2	SAP	16,0	1	16,3
3	IBM	13,9	3	14,3
4	Siemens	10,8	4	14,2
5	Fraunhofer	8,8	6	10,0
6	BMW	8,0	5	10,5
7	Microsoft	7,4	7	8,0
8	Apple	7,1	8	7,1
9	Porsche	6,9	9	6,8
10	Electronic Arts	6,3	–	–

Nennungen in Prozent

Quelle: Trendence Institut, 08/2008

IT-Freiberufler: Höhere Stundensätze

Selbstständige IT-Experten profitieren weiterhin vom Fachkräftemangel. Zumindest weist die aktuelle Statistik des Projektportals Gulp abermals eine Erhöhung für die durchschnittlich geforderten Stundensätze von 70,50 € im Februar auf nunmehr 71,20 € im August aus. Im Vergleich zum Vorjahr gibt es mehr Freiberufler, die Stundensätze über 70 € fordern. Bei der Gruppe mit Forderungen ab 110 € sind die Zuwächse am stärksten ausgeprägt (+26,4 %). Zugleich ist der Anteil derer gesunken, die sich mit weniger als 70 € pro Stunde begnügen. Die größte Gruppierung (24,3 %) forderte im August Stundensätze zwischen 70 und 79 €. Für alle Positionen konnte Gulp eine Steigerung der Stundensatzforderungen beobachten.

Stundensatzforderungen

Position	1.02.2007	1.08.2007	1.02.2008	1.08.2008
Softwareentwickler	62	63	64	66
Berater	72	73	74	75
Trainer	65	66	67	68
Projektleiter	74	76	78	78
Administrator	54	55	55	56
Qualitätssicherung	61	62	63	64

Alle Angaben in Euro

Quelle: Gulp, 09/2008



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

KURZ NOTIERT

Spendierfreudig: Microsoft beabsichtigt in den kommenden fünf Jahren bis zu 40 Mrd. Dollar für den Rückkauf eigener Aktien springen zu lassen. Auch wird die kommende Quartalsdividende mit 13 Cent um 18 % beziehungsweise 2 Cent höher ausfallen als ursprünglich beabsichtigt. Microsoft ließ in den vergangenen fünf Jahren rund 115 Mrd. Dollar für Aktienrückkäufe und Dividenden springen.

Rückkauf: Hewlett-Packard macht es Microsoft nach und kauft in großem Stil eigene Aktien zurück. Einer Meldung des IT-Konzerns zufolge hat der Verwaltungsrat hierfür weitere acht Mrd. Dollar genehmigt. Bereits im November hatte HP ein Rückkaufprogramm mit gleichem Umfang initiiert. Momentan sind rund 2,5 Mrd. HP-Aktien im Umlauf.

Handstreich: HP plant die Akquisition von Lefthand Networks, einem Anbieter von Lösungen für die Speicher-Virtualisierung und für iSCSI-basierende SAN (Storage Area Networks). Für den Kauf nimmt der US-Konzern 360 Mio. Dollar in die Hand. Bis Ende Januar kommenden Jahres soll die Übernahme vollzogen sein. Danach soll das Geschäft von Lefthand Networks in HPs Storageworks-Division des Geschäftsbereichs TSG (Technology Solutions Group) integriert werden.

Aufkauf: Quest Software hat für circa 79 Mio. Dollar Cash die Netpro Computing übernommen. Die Netpro-Produkte sollen Quests Lösungsportfolio mit Anwendungen für die einfachere Migration, Verwaltung und Sicherung von Microsofts Active-Directory-, Exchange-, Sharepoint- und SQL-Server-Umgebungen komplettieren. Ein endgültiger Fahrplan soll noch im Oktober vorliegen.

Marktforscher sagen über 5 % IT-Wachstum voraus

An der Billionen-Grenze

Achim Born

Die Nachfrage nach IT steigt weltweit nach wie vor kräftig. Nach aktuellen Daten des Marktforschungsinstituts EITO wächst der Weltmarkt heuer voraussichtlich um 5,2 % auf 963,5 Mrd. Euro.

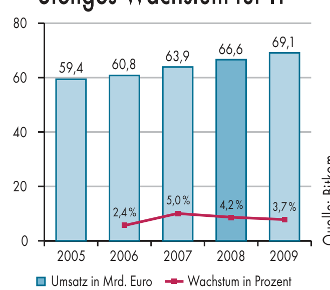
Der Konjunktureinbruch und steigende Rohstoffpreise hinterlassen noch keine Spuren in der IT-Industrie. Das meldet zumindest das EITO (European Information Technology Observatory). Nach der buchhalterischen Fleißarbeit der Marktbeobachter werden die weltweiten Umsätze mit Informationstechnik in diesem Jahr um 5,2 % zulegen. Für 2009 liegt das prognostizierte Plus mit 5,6 % sogar noch ein wenig über dem aktuellen Wachstumsniveau. Dann könnte der Umsatz mit Computern, Software und IT-Dienstleistungen weltweit erstmals die Marke von einer Billion Euro überspringen.

Den EITO-Recherchen zufolge weisen die einzelnen Regionen ein zum Teil erheblich unterschiedliches Wachstumstempo auf. Einen regelrechten Boom erleben zurzeit beispielsweise die Volkswirtschaften China, Indien und Russland mit Wachstumsraten zwischen 17 und 18 %. So wächst in China der IT-Markt um 17,8 % auf 39,1 Mrd. Euro. In Indien wird ein Plus von 17,2 % auf 18 Mrd. Euro erwartet und für Russland 17,5 % (auf dann 12,5 Mrd. Euro) gemeldet. Die Nachfrage in der Europäischen Union wird 2008 dagegen nur um 4,2 % auf 311,1 Mrd. Euro ansteigen.

Für das Wachstum sind in erster Linie die neuen EU-Mitglieder wie Polen, Tschechien oder Rumänien verantwortlich, die noch Nachholbedarf beim Ausbau ihrer IT-Infrastruktur haben. Im kommenden Jahr soll das Wachstum mit 4,1 % auf einem ähnlichen Niveau liegen. In Japan legt der Markt nach der EITO-Prognose heuer um 4,0 % auf 127,7 Mrd. Euro zu. Selbst der US-Markt wächst noch um ordentliche 3,7 % auf 345 Mrd. Euro. Im kommenden Jahr soll der Zuwachs mit 4,4 % sogar noch höher ausfallen.

Hierzulande steigt der Umsatz in der Informationstechnik laut einer Meldung des Bitkom mit einem Wachstum von 4,2 % auf dann 66,6 Mrd. Euro. Wie in den vergangenen Jahren sind wieder einmal die Bereiche Software und IT-Dienste die entscheidenden Wachstumstreiber (plus 5,3 % auf 14,6 Mrd. Euro respektive 6,3 % auf 32,7 Mrd. Euro). Der Umsatz mit PCs steigt nach Bitkom-Berechnungen um 2,1 % auf 6,7 Mrd. Euro. Dafür müssen die Hersteller allerdings auch 11,6 Mio. Systeme verkaufen, 1,5 Mio. beziehungsweise 15 % mehr als im Vorjahr. Darunter befinden sich 7,2 Mio. Notebooks (+26 %). Desktops bleiben mit 4,4 Mio. Stück etwa auf dem Niveau des Vorjahres.

Im Unterschied zum IT-Markt sinkt der Umsatz in der Telekommunikation im laufenden Jahr voraussichtlich um 1,2 % auf 66,5 Mrd. Euro. Besser als erwartet läuft dagegen das Geschäft mit digitaler Konsumentenelektronik. Der Umsatz wird voraussichtlich um 5,4 % auf 12,4 Milliarden Euro zulegen. Im Frühjahr war der Bitkom noch von plus 2,4 % ausgegangen. Der Lobbyverband der IT-Industrie rechnet mit Blick auf den gesamten ITK-Markt mit einem Plus von 1,8 % auf 145, 5 Mrd. Euro. Auch hier lag die Prognose zu Jahresbeginn niedriger, wenn auch nur um 0,2 Prozentpunkte. Für das kommende Jahr rechnet der Lobbyverband allerdings nur noch mit einem Wachstum des Gesamtmarktes in Höhe von 1,5 %. Hier war man zu Jahresbeginn noch optimistischer – seinerzeit wurden 2 % prognostiziert.



Getrieben durch Software und Dienstleistungen: andauerndes Wachstum im deutschen ITK-Markt

Online-Werbemarkt trotzt Konjunktur-Flaute

Der weltweite Markt für Onlinewerbung erreicht einen neuen Höchstwert. Nach aktuellen Daten des Marktforschungsinstituts EITO wächst der Umsatz im laufenden Jahr voraussichtlich um 23 % auf 31,7 Mrd. Euro. Überdurchschnittlich legen die Online-Werbeausgaben in Europa und weiten Teilen Asiens zu. In der EU sollen das Plus 31 % und die Einnahmen 9,1 Mrd. Euro betragen. Die USA bleiben weiterhin der mit Abstand größte Markt für Internetwerbung, trotz der Finanzkrise soll das Wachstum 13 % betragen. Das Online-Werbeaufkommen erreicht damit ein Volumen von 13,6 Mrd. Euro. Kräftig zulegen soll der Umsatz in China mit plus 46 % auf 1,2 Mrd. Euro. Der japanische Markt für Internetwerbung wächst um 15 % auf 3,3 Mrd. Euro. Zm Vergleich: Die weltweiten Umsätze mit Fernsehwerbung werden sich dem EITO-Vorhersagen zufolge in diesem Jahr mit plus 8 % auf ein Volumen von 139 Mrd. Euro einpendeln.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Deutschland: Miese Noten als IT-Standort

Eine aktuelle Studie der Economist Intelligence Unit (EIU) zeigt auf, was die Schwächen bei Forschung, Entwicklung und Bildung für Deutschland im Ländervergleich bewirken. Demnach verliert die Bundesrepublik in der Rangfolge der Attraktivität für die IT-Industrie weiter an Boden und ordnet sich gegenüber der Vorjahresuntersuchung drei Ränge niedriger auf Platz 19 ein. Die Bedingungen für die IT-Industrie gelten der EIU zufolge europaweit vor allem in Skandinavien, Großbritannien (Platz 3), den Niederlanden (Platz 10) und der Schweiz (Platz 11) als günstiger. Weltweit führten die USA die Rangliste an, gefolgt von Taiwan.

Schwächen im wirtschaftlichen und rechtlichen Umfeld, der Infrastruktur und bei Innovationen hemmen das Wachstum der Branche in den Schwellenländern Indien, China und Russland, die auf den Rängen 48 bis 50 liegen. Die EIU-Analyse basiert auf einer Bewertung der Faktoren Forschungs- und Entwicklungsgemeinschaft, IT-Infrastruktur, Rechtssystem, gesamtwirtschaftliches Umfeld, Bildung/Angebot an qualifizierten Fachkräften sowie der staatlichen Unterstützung für die IT-Branche. Dazu werden die genannten Faktoren wie folgt gewichtet: Forschungs- und Entwicklung 25 %, IT-Infrastruktur 20 %, rechtliches Umfeld 10 %, gesamtwirtschaftliches Umfeld 10 %, das Angebot an qualifizierten Fachkräften 20 % sowie die staatliche Unterstützung für das Wachstum der IT-Branche 15 %.

Best Buy: Napster übernommen

Für insgesamt 121 Mio. Dollar übernimmt die US-Handelskette Best Buy den Onlinedienst Napster. Der Kauf soll im vierten Quartal abgeschlossen sein. Dabei wechseln der 700 000 Kunden starke Abostamm, die webbasierte Kundendienst-Plattform sowie mobile Dienste den Eigner. Napster war 1988 als Tauschbörse für MP3-Dateien gegründet worden. Die dabei genutzte Peer-to-Peer-Technik galt seinerzeit als revolutionär, kam wegen illegaler Downloads jedoch in Verruf. Heute müht man sich, mit legalen Geschäften zu überleben, unter anderem per Flatrate-Angeboten für legalen Zugriff auf Onlinemusik.

Gartner-Prognose: Indien boomt

Ein äußerst robustes Wachstum von durchschnittlich 14,8 % jährlich bis 2012 prognostiziert Gartner für den indischen ITK-Markt. Allein in diesem Jahr sollen die Ausgaben um 17,2 % auf 64,7 Mrd. Dollar anschwellen. Vergleichbar zu den etablierten Märkten wie USA und Europa wird das Wachstum insbesondere durch die Segmente Software und IT-Services angetrieben. Das Hardwaregeschäft soll sich ebenfalls überdurchschnittlich entwickeln.



Sicheres Geschäft: McAfee sichert sich Secure Computing. Für den Netzwerksicherheitsspezialisten will man insgesamt 465 Mio. Dollar auf den Tisch legen. Die Akquisition muss allerdings noch von den zuständigen Behörden und den Secure-Computing-Aktionären genehmigt werden. Das Management von McAfee rechnet damit, dass bis Ende des Jahres die Übernahme abgeschlossen ist.

Einkauf: Oracle kauft Advanced Visual Technology (AVT). Die britische Firma ist Hersteller von Planungssoftware für Verkaufsräume und -regale. Unter anderem bietet sie Software zum Planen von Ladengeschäften und Regalen in 3D-Darstellung. Über den Kaufpreis wurde nichts bekannt.

Internetzugang per Handy gewinnt Freunde

16 % der Deutschen nutzen laut einer Studie von TNS Infratest das mobile Internet (rund 10,4 Mio. Personen ab 14 Jahren). Betrachtet man allein den E-Mail-Empfang oder Versand, sind es 12 %, die diesen Service nutzen. Drei Viertel dieser Nutzer bedienen sich hierzu eines Push-Dienstes, zwei Fünftel gehen auf die Website ihres Anbieters, um die Mails zu „checken“. 55 % der Nutzer mobiler Internet-Services lesen WAP-Seiten, die speziell für die Nutzung mit dem Handy optimiert sind. Normale HTML-Seiten nutzen nahezu drei Viertel der Befragten. Nach Auskunft von TNS Infratest dominiert bei der Nutzung der Aufruf von Suchmaschinen. Häufig werden zudem Nachrichten, Sportinformationen oder das Wetter abgerufen. Sogenannte Web 2.0-Anwendungen wie Social-Networking-Seiten und Videoportale steuert dagegen bislang nur eine Minderheit an.

sd&m heißt jetzt Capgemini

Seit dem 1. Oktober tritt sd & m gemeinsam mit der SAP-Business-Solutions-Einheit von Capgemini in Deutschland und der Schweiz unter der Bezeichnung Capgemini sd & m auf. Bislang durfte das Münchener Softwarehaus, obgleich es seit 2001 zu 100 Prozent der französischen Capgemini gehört, noch unter eigener Marke auftreten. Dabei konzentrierte sich sd & m in erster Linie auf das angestammte Geschäft der Individualentwicklung. Wie der sd & m-Chef Edmund Küpper in Interviews bemerkte, war SAP in der Vergangenheit immer „ein Feind“, der den Anwendern Standardsoftware ans Herz legte. Allerdings hatte sd & m 2006 mit der Plecto AG einen ausgewiesenen Spezialisten für SAP-Technologie übernommen. Mit diesem wollte man das eigene Angebot an maßgeschneiderten IT-Lösungen in die SAP-Systemwelt ausweiten.

Zu Beginn des Jahres wurden die SAP-Netweaver-Spezialisten von sd & m mit Capgemini-Beratern aus dem Process & Application Consulting dann zu eigenen Einheiten unter dem Dach der Capgemini-Gruppe zusammengeführt. Nun geht diese wieder mit sd & m zusammen. Bei der neuen Einheit sind rund 2000 Mitarbeiter an zehn Standorten in Deutschland und der Schweiz beschäftigt, rund 1400 von sd & m.

Accenture erfolgreich

IT-Service-Spezialist Accenture blickt auf ein erfolgreiches Geschäft zurück. Die Bilanz des im August beendeten Geschäftsjahrs weist einem Umsatz von 23,39 Mrd. Dollar (+19 %) aus. Die Beratungssparte steuert auf 14,12 Mrd. Dollar zu, mit Outsourcing nahm man 9,3 Mrd. Dollar ein. Der Nettogewinn wuchs um rund ein Drittel auf 1,7 Mrd. Dollar. Im Geschäftsbereich EMEA (Europa, Naher Osten, Afrika) kletterte der Umsatz um 21 % auf 11,5 Mrd. Dollar. Dabei profitiert man jedoch von der Schwäche der US-Währung. Denn auf Basis der lokalen Währungen pendelt sich das Wachstum bei rund 10 % ein.

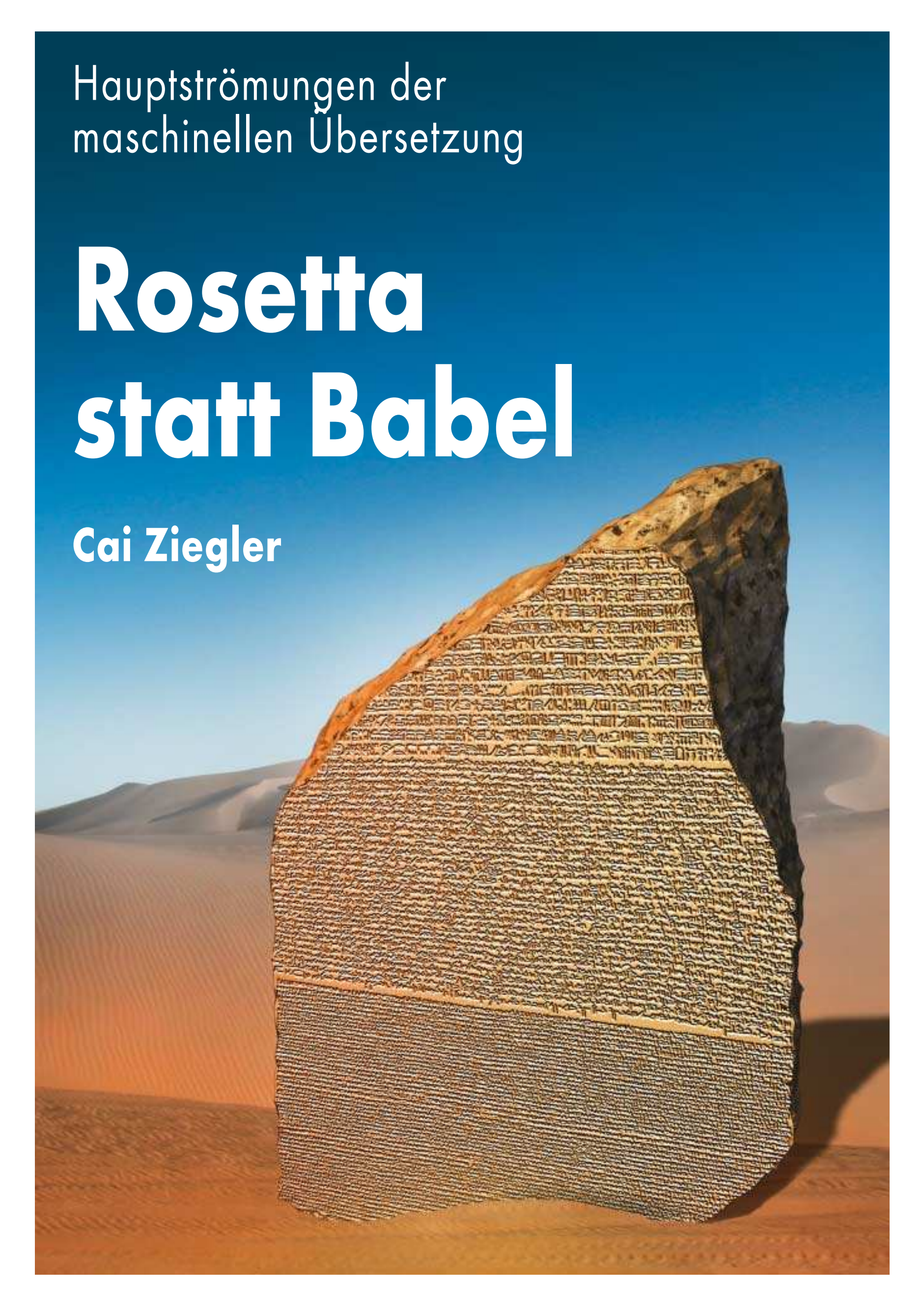
SAP hilft Innocentive

SAP hat eine Partnerschaft mit Innocentive angekündigt. Gleichzeitig wird das Walldorfer Unternehmen über den SAP Netweaver Fonds in das Unternehmen investieren. Die Onlineplattform von Innocentive ist ein weltweites Forum, in dem Experten aus allen Branchen und Regionen kooperieren, um innovative Lösungsansätze für Unternehmen in besonders forschungsintensiven Bereichen zu entwerfen. Mehr als 160 000 Ingenieure, Wissenschaftler, Erfinder, Unternehmer und Forschungsorganisationen aus über 175 Ländern beteiligen sich an diesem „interaktiven Think Tank“. Die besten Ergebnisse werden prämiert.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Hauptströmungen der maschinellen Übersetzung

Rosetta statt Babel

Cai Ziegler

Die maschinelle Übersetzung von Texten ist eins der ältesten Versprechen der künstlichen Intelligenz. Zwar liegt dessen Erfüllung noch in weiter Ferne, doch bringen Ansätze aus der Sprachstatistik neues Leben ins Spiel.

„Zwei Seelen wohnen, ach! in meiner Brust“ – auf wenige Gebiete der Informatik lässt sich dieser gern zitierte Satz aus Goethes Faust besser anwenden als auf die maschinelle Übersetzung, bei der sich seit nahezu zwei Jahrzehnten Computerlinguisten und Anhänger der Sprachstatistik erbitterte Grabenkämpfe liefern. Denn tatsächlich sind die beiden grundverschieden und lassen nur wenig Raum für Überlappungen: Während die Linguisten regelbasierte Übersetzer bauen, bei denen grammatikalische Regeln in mühevoller Kleinarbeit per Hand für jede zu übersetzende Sprache modelliert werden müssen, verfolgen die Statistiker einen gänzlich anderen Ansatz: Sie bemühen weder Wörterbücher noch Grammatikregeln. Stattdessen lernt die Maschine diese Gegebenheiten von selbst, anhand so genannter paralleler Textcorpora – großer Textmengen, die denselben Inhalt in zwei Sprachen zum Ausdruck bringen. Die Gesetzestexte der EU sind ein gutes Beispiel für parallele Corpora. Oder eben der bekannte Stein von Rosetta, wobei das Kriterium der Korpusgröße in diesem Fall nicht erfüllt ist.

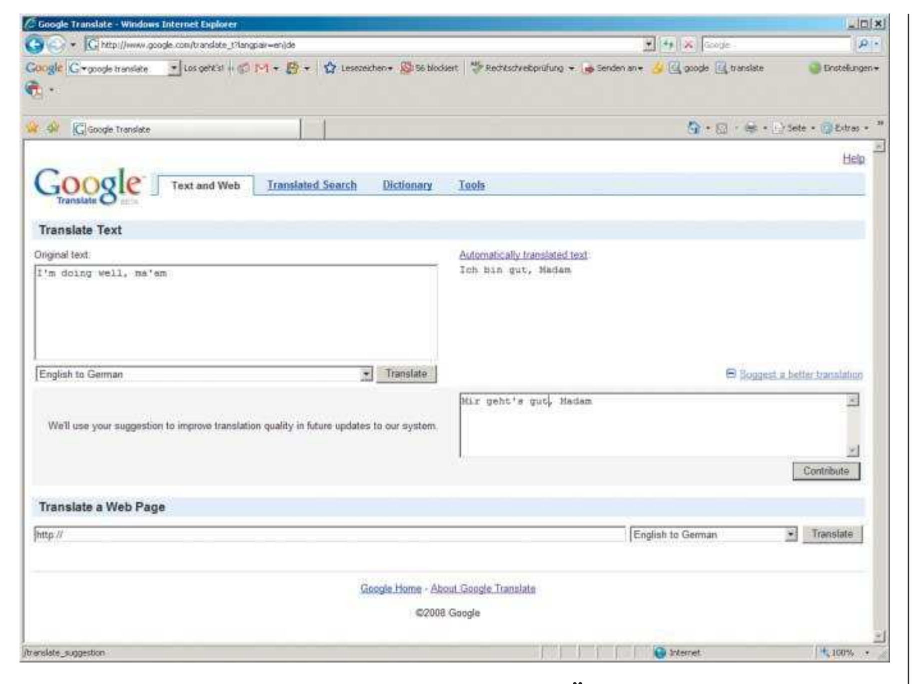
Allmählich scheint sich das Blatt zugunsten der Sprachstatistiker zu wenden, die bislang zwar im Bereich der Forschung ihren Platz sichern und in diversen Benchmarks mit guten Ergebnissen aufwarten konnten, aber in puncto kommerzieller Erfolge nur wenig vorzuweisen hatten: Nahezu alle Anbieter von Produkten zur Übersetzung verschiedensprachiger Texte sehen sich der regelbasierten Computerlinguistik verbunden. Google hat vor etwas mehr als zwei Jahren die Entscheidung gefällt, sich aktiv in das Geschehen einzubringen.

Verließ sich der Primus der Suchbranche bis dahin zur Übersetzung von Webseiten auf die Software von Systran, einer französischen Firma, die als Urahn der maschinellen Übersetzung gelten darf, so ist dem seit Oktober 2007 nicht mehr so: Google hat den Dienst durch selbst gestrickte Software ersetzt, die im Gegensatz zu Systran rein auf Sprachstatistik fußt (siehe Abb. 1). Die Umstellung erfolgte ohne großes Aufheben und fand ihren Niederschlag hauptsächlich in einigen Blogs, die sich jedoch kritisch zu den erzielten Resultaten äußerten. In Kommentaren bemängelten einige, dass sich die Qualität der Übersetzung nicht wesentlich von der Systrans unterschied.

Fit in Arabisch und Chinesisch

Das mag stimmen, wie eigene Fingerübungen dem Leser schnell vor Augen führen dürften. De facto sollte die Sichtweise jedoch nicht die des halbleeren Glases, sondern die des halbvollen sein: In weniger als zwanzig Jahren, denn tatsächlich begann die Forschung sich erst Anfang der Neunziger mit statistischen Übersetzungsverfahren zu beschäftigen, zog der neue, auf Wahrscheinlichkeiten gründende Ansatz mit den in fünf Dekaden gereiften linguistischen Verfahren gleich. Darüber hinaus hat der Neuankömmling die alte Garde in einigen Sprachen schon überholt: Das National Institute of Standards and Technology (NIST) veranstaltet alljährlich einen

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Das nun statistische Google Translate liegt bei der Übersetzung nicht immer richtig, ermöglicht jedoch die Eingabe einer Korrektur bei fehlerhaften Resultaten (Abb. 1).

Wettbewerb, bei dem sich Systeme zur maschinellen Übersetzung miteinander messen können.

In den Jahren 2005 und 2006 – neuere Ergebnisse liegen noch nicht vor – hat Googles eigener Ansatz in den Kategorien Arabisch – Englisch und Chinesisch – Englisch die anderen Konkurrenten deutlich hinter sich gelassen (siehe Kasten), darunter 2005 auch Systran, das jedoch 2006 gar nicht mehr antrat. Dass sich dieser Erfolg nur auf die beiden genannten exotischeren Sprachen bezog, ist darin begründet, dass ausschließlich diese Sprachkombinationen für den Benchmark betrachtet wurden.

Es ist eine durchaus berechtigte Frage, warum sich die maschinelle Übersetzung als ein derartiges Stiefkind der Informatik erweist. Dabei schien man der Lösung schon so nah zu sein: Zu Zeiten des Kalten Krieges, im Jahre 1954, führten Wissenschaftler von IBM in einem heute als Georgetown-Experiment bekannten Feldversuch erfolgreich ein Rechensystem vor, das etwa 60 russische Sätze ins Englische übersetzte. Der Erfolg schlug geradezu haushohe Wellen und führte dazu, dass sich Politik, Militär und Forschung am Gedanken der vollständig maschinellen Übersetzung geradezu berauschten. Leon Dostert, ein renommierter US-Professor, verkündete vollmundig, dass maschinelle Übersetzung schon in drei bis fünf Jahren ein gelöstes Problem sei. Damit lag er offenkundig falsch.

Direkte Übersetzung mit Regelwerken

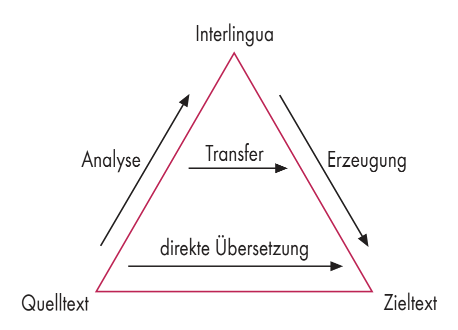
Jenes frühe, von IBM entwickelte System gilt als Vertreter der sogenannten direkten Übersetzung: Ein Text der Quellsprache wird ohne Umweg über eine abstrakte Darstellung in die Zielsprache überführt. Zum Handwerks-

iX-TRACT

- Regelbasierte Ansätze, die enormes Expertenwissen erforderten und nur unzulängliche Ergebnisse lieferten, haben die maschinelle Übersetzung viele Jahrzehnte dominiert.
- Seit den Neunzigern erleben statistische Ansätze der maschinellen Übersetzung ihre Blütezeit, die weder Wörterbücher noch Expertenwissen benötigen.
- Stützpfeiler dieser neuen Herangehensweise sind Paralleltexte in rauen Mengen, aus denen die Maschine schließlich Modelle zur Übersetzung lernt.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Die regelbasierten Ansätze weisen verschiedene Abstraktionsstufen auf, die vom betrachteten Sprachpaar losgelöst in eine Zwischensprache überführen (Abb. 2).

zeug bei dieser Vorgehensweise zählen massive Wörterbücher, die eine Übersetzung Wort für Wort ermöglichen. Weitere essenzielle Ingredienzen sind Regeln für die morphologische Analyse, um deklinierte Formen von Substantiven und Adjektiven sowie konjugierte Verben auf die Stammform zurückführen zu können. Dadurch weiß der Rechner, dass „hob“ und „gehoben“ auf das Verb „heben“ zurückzuführen sind. Hinzu kommen Regeln zur syntaktischen Vorverarbeitung. Diese umfassen das Auflösen von Komposita. Vor allem im Deutschen und Finnischen ist das nicht trivial, da in beiden Sprachen die morphosyntaktische Vielfalt reich ist. Der Donaudampfschifffahrts… lässt grüßen.

Da eine reine Übersetzung der Wörter wenig Sinnreiches hervorbrächte, sind derartige direkte Übersetzer zudem mit einigen simplen grammatikalischen Regeln ausgestattet, die sich beispielsweise der Satzstellung annehmen. Im Deutschen findet sich das Prädikat tendenziell am Ende eines Satzes, was für viele anderen Sprachen nicht gilt: „Ich habe das Ende der Straße gesehen“ entspricht im Englischen „I have seen the end of the road“. Eine Nichtbeachtung der Stellung des Verbs würde somit in beiden Richtungen zur Erzeugung eines Satzes führen, der grammatikalisch schlicht falsch wäre.

Direkte Übersetzung funktioniert immer nur für genau das Sprachpaar, für das sie entworfen wurde. Ein Transfer für andere Paare erfordert eine mühselige Anpassung der Regeln sowie das Vorhandensein entsprechender Wörterbücher. Die Qualität ist nicht das Gelbe vom Ei, und so folgte 1966, nach über zehn Jahren intensiver Forschung, das Eingeständnis, dass maschinelle Übersetzung nicht so leicht zu haben sei wie angenommen.

Wer übersetzt am besten im ganzen Land?

Alljährlich richtet das in den USA ansässige National Institute of Standards and Technology, kurz NIST, einen Wettbewerb aus, bei dem Anbieter von Softwaresystemen zur maschinellen Übersetzung gegeneinander antreten. Die Teilnahme ist kostenlos. In den letzten Jahren hat die Zahl der sich dem Vergleich stellenden Firmen und Universitäten nahezu exponentiell zugenommen, was auf ein drastisch gestiegenes Interesse am Thema hindeutet. Ausgangsbasis der Evaluation stellen dabei vom NIST vorgegebene Texte in ausgewählten Sprachen dar, die von den Aspiranten ins Englische zu übersetzen sind. In den Jahren 2005 und 2006 waren dies Arabisch und Chinesisch.

Alle Teilnehmer lassen ihre Systeme auf die präsentierten Texte los und senden das Ergebnis zurück zur NIST. Die Validität der Ergebnisse ist somit stets unter der Prämisse zu sehen, dass keiner der Wettbewerber schummelt. Beim NIST beurteilen Experten die Übersetzungen durch Anwendung eines unter dem Namen BLEU (Bilingual Evaluation Understudy) bekannten Bewertungssystems. Der Fokus gilt dabei zum einen der Genauigkeit der Übersetzung (= der singgemäßen und vollständigen Wiedergabe des Gesagten) wie der Fähigkeit des Systems, diese Aussagen in eine flüssige und sprachgewandte Übersetzung zu verpacken. So mancher mag bei diesen Worten mit Schaudern an die Übersetzungen römischer Dichter im Lateinunterricht zurückdenken, die zwar sinngemäß gewesen sein mögen, aber meist mehr als holprig klangen.

Neben der menschlichen Bewertung findet zudem noch eine automatisierte statt, bei der die Auftrittshäufigkeit von Sequenzen von Wörtern und Interpunktionszeichen im Hinblick auf Referenzübersetzungen gemessen wird (siehe [1]). Jenes von IBM vorgeschlagene, maschinelle Vergleichsverfahren legte in Tests ein Verhalten an den Tag, das dem menschlicher Schiedsrichter nahekommt.

Um einen Vergleichswert anführen zu können, der praktisch die maximal erreichbare Güte vorgibt, wurde BLEU auch auf menschliche Übersetzungen angewandt. Gute Übersetzer erreichten dabei für Arabisch und Chinesisch Ergebnisse zwischen 0,7 und 0,85, wobei der theoretisch erreichbare Maximalwert mit 1 angesetzt ist. Ergebnisse der maschinellen Übersetzer sind in der Tabelle rechts exemplarisch aufgeführt.

Interessanterweise funktioniert Systran, das schon 1969 das Licht der Welt erblickte und heute als das wohl am weitesten verbreitete und genutzte System gelten dürfte, noch immer nach diesen Prinzipien.

Die Sprache in der Mitte

Übersetzung ist für Menschen ebenso wenig trivial wie für Maschinen. Der Mensch muss den Text tatsächlich verstehen und sozusagen die Gedanken des Autors lesen. Nur so kann er Mehrdeutigkeiten auflösen, die bei Wörtern mit mehr als einer Bedeutung gegeben sind: Das englische „bank“ kann im Deutschen je nach Kontext das Ufer eines Flusses, den Ort, an den man Geld bringt, wie auch die Kurvenlage eines Flugzeugs bezeichnen. Noch schwieriger gestaltet sich die Herstellung des Bezuges durch Personalpronomina wie „er“ über Satzgrenzen hinweg.

Diese Stolpersteine versuchte die Forschung durch ein Festhalten an der mit der direkten Übersetzung begonnenen Strategie meistern: Wenn man eine Sprache und deren Transfer in eine andere durch hinlänglich komplexe Regeln unterfüttert, wird die Übersetzung irgendwann ausreichend gut. Also bekamen Heerscharen von Linguisten die Aufgabe, Spracheigenheiten zu modellieren.

Es folgten fünfzig Jahre Forschung, die vor allem der regelbasierten Übersetzung ihr Augenmerk widmete. Diese setzt vor allem auf der Idee der Interlingua auf: eine Repräsentation der Semantik eines Textes in einer abstrakten Zwischensprache, aus der der Zieltext generiert werden kann. Der Vorteil besteht darin, dass zum einen das Diktat einer wörtlichen Übersetzung des Quelltextes entfällt, denn es kommt rein auf die Erhaltung des Sinns an. Zum anderen muss nicht mehr für jedes einzelne Sprachpaar ein eigener Übersetzer gebaut werden; es genügt, für jede Sprache ein Modul zu konzipieren, das einen in ihr abgefassten Text in die Interlingua überführt (Analyse) sowie aus der Interlingua in die Zielsprache leitet (Erzeugung).

Ein Zwitter zwischen dem Interlingua-Ansatz und der direkten Übersetzung ist der Transfer: Dort gibt es zwar ebenfalls eine Zwischenrepräsentation, aber sie enthält noch immer Wissen, das sich auf die Auflösung von Ambiguitäten bezieht, die inhärent für das

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

gegebene Sprachpaar sind. Den Zusammenhang zwischen den diversen regelbasierten Ansätzen verdeutlicht Abbildung 2.

Viel hilft viel beim Lernen

Während sich die linguistischen Übersetzungsverfahren ohne sonderliche Höhen und Tiefen durch die Jahrzehnte schleppten, gelang Anfang der Neunziger ein Quantensprung: Eine IBM-Forschungsgruppe des renommierten Watson-Labors setzte einen sprachstatistischen Ansatz um, der alle Regeln und jegliches von Experten modellierte Wissen einfach über Bord warf und stattdessen rein auf Paralleltexte – in verschiedenen Sprachen vorhandene Dokumente – setzte (siehe [2]). Damit lassen sich Übersetzungssysteme bauen, ohne dass deren menschliche Konstrukteure die Quell- und Zielsprache überhaupt verstehen müssen. Mitarbeiter des Information Sciences Institute der University of Southern California haben derartige Ansätze beispielsweise erfolgreich zur Erforschung von Hieroglyphen und alten Schriften eingesetzt, die bislang Historiker und Sprachforscher vor Rätsel stellten (siehe [3]).

Statistische Verfahren waren zwar in der Vergangenheit des Öfteren sporadisch ausprobiert worden, allerdings ohne nennenswerte Erfolge zu verbuchen. Dass ausgerechnet jetzt die Zeit für derartige Verfahren reif war, lag unter anderem daran, dass die Rechner schneller waren und das Web seinen Siegeszug antrat. Denn durch das globale Netz standen plötzlich große Mengen von Paralleltexten zur Verfügung.

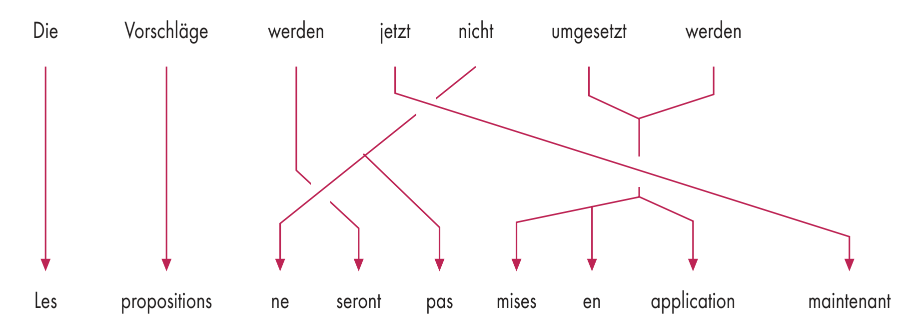
Ein beliebter Quell für Paralleltexte sind beispielsweise die meist in verschiedenen Sprachen abgefassten Firmenseiten großer Konzerne. Der wohl

NIST-Ergebnisse 2006 für Arabisch-Englisch

Rang	System	BLEU-Score
1	Google	0.4281
2	IBM	0.3954
3	Information Sciences Institute	0.3908
4	RWTH Aachen	0.3906
5	Applications Technology Inc.	0.3874
6	Language Weaver	0.3741
7	BBN Technologies	0.3690
8	NTT Communication Science Laboratories	0.3680
9	ITC-irst (Italien)	0.3466
10	Carnegie Mellon University / Univ. Karlsruhe	0.3369

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Korrespondierende Wörter können in der Übersetzung an gänzlich anderen Stellen im Satz zu liegen kommen, wie hier für eine deutsch-französische Übersetzung (Abb. 3).

„parallelste“ aller Texte dürfte zweifelsfrei die in satte 405 Sprachen übersetzte Bibel sein. Ebenso gut geeignet sind UN-Dokumente und Gesetzestexte der EU, die in alle Sprachen der Europäischen Union übersetzt werden müssen. Generell gilt bei der maschinellen Übersetzung das Paradigma „viel hilft viel“. Denn je mehr parallele Corpora vorhanden sind, desto besser ist schließlich die Qualität der Übersetzung. Vorsicht: Übersetzungen statistisch operierender Systeme liefern meist nur bei Texten gleichen Typs eine überzeugende Leistung. Ein vornehmlich auf juristische Texte trainiertes System dürfte sich nur schwerlich auf Erlebniserzählungen anwenden lassen.

Hinter dem Algorithmenvorhang

Zur Übersetzung eingesetzte Algorithmen sind nicht gerade leichte Kost, die Intuition dahinter lässt sich hingegen in populärwissenschaftlicher Form recht anschaulich darlegen.

Der erste Schritt beim Trainieren eines statistischen Übersetzers besteht in der getrennten Betrachtung beider sich entsprechender Corpora, beispielsweise des englischen und seines deutschen Pendants. Für jede dieser beiden Textkollektionen erstellt die Maschine nun ein Sprachmodell, das Vorhersagen über die Anordnung von Wörtern in Sätzen zu treffen vermag. Dies funktioniert gut, da die Mengen an Dokumenten riesig sind und diese somit den gängigen Gebrauch der Sprache geeignet widerspiegeln und abdecken. Das Sprachmodell arbeitet dabei auf Basis von n-Grammen: Satzfragmenten aus maximal n Wörtern. Daraus lässt sich beispielsweise ableiten, dass auf „schönes“ mit höherer Wahrscheinlichkeit „Auto“ folgt als umgekehrt. Oder dass das wahrscheinlichste Wort, das auf „herzliche“ folgt, „Grüße“ ist. Der Einsatz derartiger Modelle lässt sich heute schon bei Mobiltelefonen beobachten, die auf diese Weise dem Nutzer das mühselige Tippen von Kurzmitteilungen erleichtern sollen.

Anschließend erfolgt die Ausrichtung (Alignment) sich entsprechender Sätze im betrachteten Sprachpaar: Welcher Satz im deutschen Korpus entspricht welchem in der englischen Übersetzung? Dies ist aus zwei Gründen kein einfaches Unterfangen: Zum einen arbeiten die statistischen Übersetzer ohne Wörterbuch – es liegen deshalb keine groben Anhaltspunkte bezüglich der Korrespondenz von Wörtern vor, die zur Identifizierung des gesuchten Satzes dienen könnten. Zum anderen sind Übersetzungen oft nicht gänzlich wörtlicher Natur, was häufig dazu führt, dass ein Satz in der Quellsprache in zwei oder mehreren Sätze der Zielsprache mündet.

Ganz ohne Wörterbuch

Die erfolgreiche Durchführung des Alignments erlaubt das Erlernen eines weiteren Modells, das als Translation Model bekannt ist. Kommt beispielsweise in der deutschen Version das Wort „Auto“ signifikant oft genau dann vor, wenn im entsprechenden englischen Satz das Wort „car“ auftritt, so ist dies ein stichhaltiges Indiz dafür, dass „car“ die Übersetzung für „Auto“ ist. Ebenso vermag das Translation Model Übersetzungen für Wörter zu erkennen, die mehr als ein Wort der Zielsprache abbilden. Beispielsweise wird aus dem deutschen „benötigen“ im Französischen ein Konstrukt aus drei Wörtern: „avoir besoin de“.

Mit Paralleltexten lassen sich zudem ohne menschliches Zutun bilinguale Wörterbücher aufbauen. Hinderlich ist dabei jedoch, dass Deklinationen oder Konjugationen des gleichen Wortes per se nicht erkannt werden. Hier müsste Wissen über die morphologischen Gesetzmäßigkeiten einer Sprache einfließen. Das Translation Model hat neben der Erkennung der jeweiligen Übersetzung eines Wortes – dies zudem Dank eines n-Gramm-Modells im richtigen Kontext – eine weitere Bedeutung: die Erkennung des Versatzes im Text der Zielsprache. So kann ein englisches Wort weit entfernt von dem deutschen Wort stehen, das es erzeugt hat (siehe Abb. 3). Dies ist eine der größten Schwierigkeiten der maschinellen Übersetzung überhaupt.

Aus den gelernten Modellen lassen sich nun für einen zu übersetzenden Satz Hypothesen für dessen Pendant in der Zielsprache bilden. Die wahrscheinlichste darunter – im Hinblick auf die Häufigkeiten der Konstrukte in den beiden Modellen – wird als tatsächliche Übersetzung ausgewählt.

Aus Beispielen lernen

Ein artverwandter Ansatz ist EBMT (Example-Based Machine Translation), der sich vor allem bewährt hat, wenn die Anwendungsdomäne, aus der die zu übersetzenden Texte stammen, häufig wiederkehrende Satzmuster aufweist. Dies ist etwa bei technischen Handbüchern der Fall. Bei EBMT stellen ebenso wie bei der statistischen maschinellen Übersetzung parallele Corpora das tragende Element des Ansatzes dar. Jeder Satz der Quellsprache wird dabei als ein gültiges Beispiel betrachtet. Der Übersetzungsprozess kommt dann einer Zerlegung des zu übersetzenden Textes in bekannte Fragmente gleich, die schließlich durch ihre entsprechende Übersetzung in der Zielsprache ersetzt werden. Hier findet ebenfalls ein Alignment der beiden Corpora als Vorverarbeitung statt.

Googles Projekt, dessen Leitung Franz Och, einem gebürtigen Erlanger, obliegt, fußt auf den beiden korpusbasierten Ansätzen und verdankt seinen Erfolg zweifelsfrei auch der Tatsache, dass die Firma einen recht einfachen Zugriff auf viele Mengen paralleler Corpora hat. Seit Kurzem kristallisiert sich jedoch ein weiteres statistisches Verfahren heraus, das ohne diese Paralleltexte auskommt: Meaningful Machines, ein kleines Start-up an der Ostküste der USA, benötigt an deren Stelle eine große Menge von Dokumenten in der Ziel-

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

sprache, eine kleine Menge an Texten der Quellsprache, sowie ein enorm umfangreiches Wörterbuch, in dem alle Flexionen der Substantive, Adjektive und Verben aufgeführt sind (siehe [4]). Nach eigenen Angaben sei der BLEU-Score (siehe den Kasten „Wer übersetzt …“) geradezu phänomenal, doch muss diese Aussage noch in unabhängigen Tests, wie eben der Evaluation durch die NIST, validiert werden. Laut Aussage von Professor Jaime Carbonell, dem Chief Science Officer von Meaningful Machines, ist ein großes Manko momentan noch die Geschwindigkeit der Übersetzung, die alles andere als berauschend sei: Die Software rechnet momentan 10 Sekunden an der Übersetzung eines Wortes herum [5].

Fazit

Die Zukunft der maschinellen Übersetzung gehört eindeutig dem statistischen Ansatz. Das hat mittlerweile sogar der Branchen-Opa Systran eingesehen, der verlauten ließ, dass er die statistischen Methoden zur Verbesserung seines regelbasierten Ansatzes nutzen wolle. Die Aussichten stehen gut für einen zweiten Frühling der maschinellen Übersetzung, denn in Zeiten des Terrorismus sind die kleinen elektronischen Helferlein wieder gefragt wie zuletzt während des Kalten Krieges. Es verwundert daher wenig, dass gerne wieder vollmundige Versprechungen in den Mund genommen werden. So sagt Kevin Knight, einer der Pioniere der statistikbasierten Übersetzung, voraus, dass schon bald die Güte menschlicher Übersetzung für alles außer Lyrik erreicht werde. Dieser Ausspruch klingt, als stamme er aus einer Zeit von vor circa 50 Jahren. Ob er sich dieses Mal bewahrheitet, bleibt abzuwarten. (hb)

DR. CAI ZIEGLER

arbeitet als Unternehmensberater bei der Boston Consulting Group.

Literatur

[1] George Doddington; Automatic Evaluation of Machine Translation Quality Using N-Gram Co-Occurrence Statistics; Human Language Technology Conference, 2002; S. 138

[2] Peter Brown et al.; A Statistical Approach to Machine Translation; Computational Linguistics 16(2), 1990

[3] How to Build a Babel Fish; The Economist, 8. Juni 2006

[4] Jaime Carbonell et al.; Context-based Machine Translation; Conference of the Association for Machine Translation in the Americas, Boston, 2006

[5] Evan Ratcliff; Me Translate Pretty One Day; Wired Magazine, Dezember 2006

Onlinequellen

Googles Sprachstatistik in Action
www.google.com/translate_t

Systran zum Vergleich
babelfish.altavista.com/tr







© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Übersetzungssoftware: Integration in Unternehmens-IT

Sprache Gewirr

Barbara Lange

Nach der jüngsten Übernahme eines Unternehmens müssen Mitarbeiter mit ihren neuen Kollegen aus Indien oder Ungarn kommunizieren und die Webdesigner die Site des Konzerns mehrsprachig anlegen. Übersetzer aus Fleisch und Blut können da kaum helfen – bleiben maschinelle Übersetzungssysteme, die aber immer wieder Anlass zu Hohn und Spott gegeben haben.

Der Bedarf an Übersetzungen nimmt zu, denn Mehrsprachigkeit gewinnt an Popularität im Zeitalter der Globalisierung, in dem internationale Wirtschaftsbeziehungen und Parlamente Berge von Text erzeugen. Trotzdem ist es nach Einschätzung von Branchenkennern nicht leicht, mit maschineller Übersetzung Geld zu verdienen. Das gilt zumindest für den Privatkundenmarkt, denn warum etwas kaufen, wenn es bei Google, Yahoo und einigen Herstellern professioneller Übersetzungssysteme wie Linguatec, Prompt oder Language Weaver kostenlose Online-Übersetzungen gibt? Seit Mitte 2008 bietet zudem Microsoft mit dem „Windows Live Translator“ eine Online-Übersetzung von bis zu 500 Wörtern beziehungsweise einer Webseite.

Für einige der 25 Sprachpaare verwendet Microsoft eine Eigenentwicklung, die statistische Methoden nutzt, in den übrigen Fällen greift das Unternehmen auf das System von Systran zurück. Wie auf dem Blog (blogs.msdn.com/translation) zu lesen ist, können Nutzer ein Translator-Add-in in ihre Webseiten und in Office integrieren.

Onlinesysteme liefern zwar eine ungenaue, manchmal zur Heiterkeit anregende Rohübersetzung – sie ist aber allemal ausreichend für ein grobes Verständnis eines Textes und gegebenenfalls für die Entscheidung, ob man ihn überhaupt gebrauchen kann.

Firmeninterna online übersetzt

Dass solche Systeme eine Sicherheitslücke in Unternehmen nach sich ziehen, zeigt Heisoft Publishing AG, hierzulande Distributor von Promt und Systran, in seiner Studie „Sicherheitslücke: Online-Übersetzung – Online-Übersetzungsdienste und IT Sicherheit im Intranet“, die *iX* vorlag.

Heisoft betreibt einen registrierungspflichtigen Online-Übersetzungsdienst auf der Basis des Systems von Systran und übersetzt täglich 15 000 bis 20 000 Texte oder Internetdokumente. Darunter fanden sich Arbeits- und Geschäftsverträge, Satzungen und andere unternehmensinterne Papiere, die Mitarbeiter ganz ungezwungen auf ihre unverschlüsselte Server-Reise um die Welt schickten. Die Empfehlung: Unternehmen sollten den Zugang zu Online-Übersetzungsdiensten kappen und die Anfragen der Mitarbeiter auf eine im Intranet installierte Version umleiten. Das kann zudem die Übersetzungsqualität erhöhen, sofern das Unternehmen eigene Termini und Standardformulierungen zentral hinterlegt – dazu später mehr.

Über den Tellerrand der kostenlosen Übersetzungsdienste hinausgeschaut, erkennt man bei den am Markt verfügbaren Systemen Unterschiede im Funktionsumfang, der mal die Ansprüche unternehmerischer Einzelkämpfer, mal die mittelständischer Unternehmen oder gar global agierender Großkonzerne decken soll.

Die Marktübersicht in diesem Beitrag konzentriert sich auf professionell einsetzbare maschinelle Übersetzungssysteme und listet einige Onlinedienste auf. Nicht enthalten sind Managementsysteme, die die Übersetzungsprozesse

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

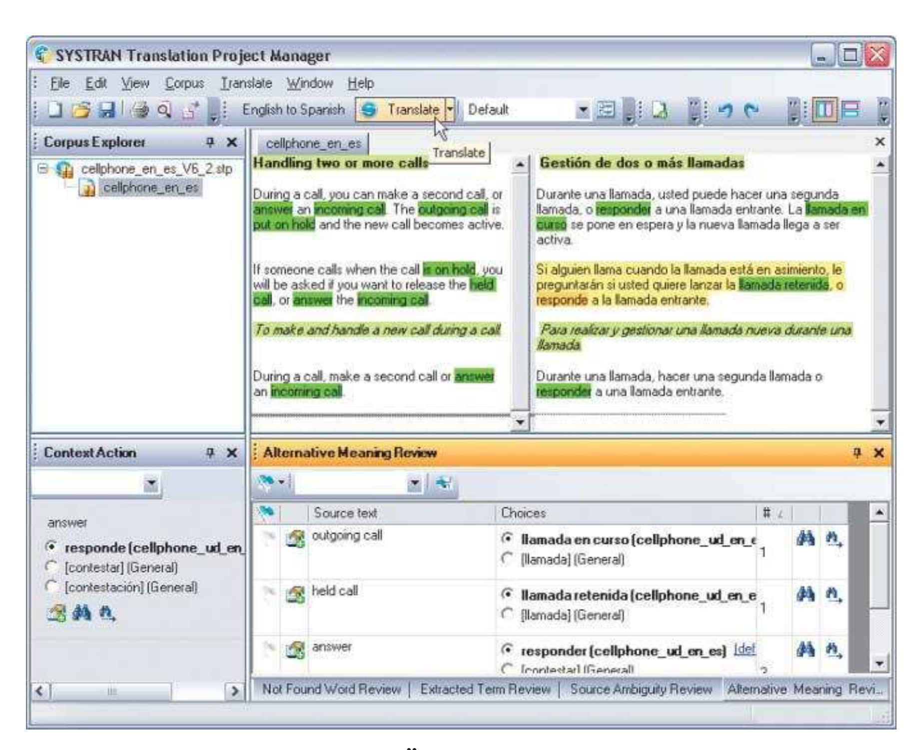
in großen Unternehmen und professionellen Übersetzungsbüros verwalten und steuern, in denen die maschinelle Übersetzungssoftware nur ein Baustein von vielen ist. Unberücksichtigt, sozusagen auf der anderen Seite bleiben elektronische Wörterbücher im Taschencomputerformat in der Übersicht. Letztlich kann trotz aller Mühe eine Marktübersicht keinen Anspruch auf Vollständigkeit erheben, denn es gibt Überschneidungen mit anderen Systemen, und der Markt verändert sich ständig.

Hybride Systeme vereinen zwei Ansätze

Wie der Artikel „Babel oder Rosetta“ im Heft beschreibt (siehe Seite 42), existieren mit regelbasierten und statistischen Methoden zwei grundlegende Ansätze der maschinellen Übersetzung. Aber vor dem Hintergrund jahrzehntelanger Forschungen übersetzen die meisten der verfügbaren Produkte aus historischen Gründen regelbasiert. Statistische Verfahren setzen derzeit nur Google, Microsoft und Language Weaver ein.

Language Weaver entstand 2002 als Spin-off der University of Southern California’s Information Sciences Institute (USC/ISI). Seit einiger Zeit übersetzt der Enterprise Translation Server von Language Weaver bis zu 300 Zeichen im System Babylon. Etwas mehr darf es bei Across sein, dort bildet er einen Bestandteil der zentralen Plattform für alle Sprachressourcen und Übersetzungsprozesse im Unternehmen Sie heißt Language Server und steuert große Übersetzungsprojekte, was den Aufwand für das Verfassen und Übersetzen von technischen Dokumentationen verringern soll.

Ziel ist eine Wiederverwendbarkeit von Übersetzungen, die das System in einem zentralen Datenpool vorhält und dem professionellen Übersetzer vorschlägt, sofern er wieder eine bekannte Passage benutzt. Wenn nicht, schlägt Language Weaver eine Übersetzung vor, die der Nutzer in den ständig mit akzeptierten Übersetzungen gefüllten Datenpool übernehmen kann.



Europaweit: Für das regelbasierte Übersetzungssystem von Systran plant die EU zusätzliche Sprachpaare (Abb. 1).

Hohe Erwartungshaltung bei Kunden abbauen

Euphorie, was die Übersetzungsqualität betrifft, kam während der Recherche bei keinem Hersteller auf. Alle betonen, dass selbst die professionellen Systeme nur Rohübersetzungen liefern und man als Erstes die hohe Erwartungshaltung potenzieller Kunden abbauen müsse. Ein Trend zeichnet sich in der Verbindung beider Ansätze zu hybriden Systemen ab, die das Beste aus beiden Welten integrieren sollen, um die Übersetzungsqualität zu verbessern.

Regelbasierte Systeme verfügen zwar über linguistisches Wissen und kennen die Grammatik einer Sprache, ihnen fehlt aber das Wissen über den Kontext von Wörtern und Sätzen, was die korrekte Übersetzung von mehrdeutigen Wörtern oder Eigennamen erschwert. Dieses „Weltwissen“ besitzen die statistischen Verfahren nach der Analyse umfangreicher Paralleltexte. Ihnen fehlt es wiederum an Regeln, mit denen sie die gefundenen Ausdrücke grammatisch richtig kombinieren können. Hybride Verfahren ergänzen das jeweils Fehlende.

Translation Memory dient als Vorlage

So baut Linguatec für seinen ursprünglich regelbasierten Personal Translator einen aus 2,5 Milliarden Wörtern bestehenden Korpus auf. Er enthält Informationen darüber, welche Begriffe in der Regel zusammen mit anderen vorkommen. Auf der Basis eines Kooperationsvertrags untersucht Linguatec Texte von Google, Nachrichten aus Zeitungen sowie Fachtexte. Darüber hinaus arbeitet Linguatec mit einem Translation Memory, das die bisherigen Übersetzungen des Unternehmens enthält und den späteren Zugriff darauf ermöglicht. Zu dem

iX-TRACT

- Hersteller und Forschungsprojekte versuchen, regelbasierte und statistische Methoden durch die Vorteile des jeweils anderen Ansatzes zu verbessern.
- Die Übersetzungsqualität lässt sich durch Terminologieverwaltungen, übersetzungsgerechtes Schreiben und Translation Memories verbessern.
- Unternehmen sollten kostenlose Online-Übersetzungsdienste wegen des hohen Sicherheitsrisikos nur zurückhaltend einsetzen.
- Die Erwartungshaltung gegenüber maschinellen Übersetzern ist oft zu hoch.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Kostenlose Online-Übersetzer

Anbieter	Produkt	Link	Methode
Abacho	Online-Übersetzung	uebersetzer.abacho.de	nutzt SW von PROMT
Babylon Ltd.	Online-Übersetzung	translation.babylon.com	nutzt SW von Language Weaver
Google	Online-Übersetzung	www.google.de/language_tools?hl=de	statistisch
Linguatec	Online-Übersetzung	www.linguadict.de	regelbasiert, ergänzt durch statistische Verfahren
Microsoft	Windows Live Translator	www.windowslivetranslator.com	nutzt Google-Übersetzung plus Eigenentwicklung (statistisch)
Promt GmbH	Online-Übersetzung	www.online-translator.com	hybrid
SDL International	Online-Übersetzung	www.freetranslation.com	hybrid
Wörterbuch.Info	Online-Übersetzung	www.woerterbuch.info/volltext-uebersetzung.php	nutzt Google
Yahoo Babelfish	Online-Übersetzung	de.babelfish.yahoo.com	Systran

Hersteller von maschineller Übersetzungssoftware

Hersteller	Produkt	Link	Methode
Babylon Ltd.	Babylon 7; Babylon enterprise	www.babylon.com/ger	nutzt SW von Language Weaver
DFKI (hostet Open-Source-System)	OpenLogos	logos-os.dfki.de	regelbasiert
Digital publishing	translate quick/plus/pro/netzwerk	www.digitalpublishing.de	hybrid
Language Weaver	Enterprise Translation Server; Custom Translation Server; Translation On Demand	www.languageweaver.com	statistisch
Linguatec Sprachtechnologien GmbH	PT 2008 NET; PT 2008 Intranet	www.linguatec.de	regelbasiert, ergänzt durch statistische Verfahren
Lucy Software and Services	Lucy Translator	www.lucysoftware.com/index_de.html	regelbasiert
Language Engineering Company 2008	Power Translator	www.lec.com	regelbasiert
Lingenio	translate pro; translate netzwerk	www.lingenio.de	regelbasiert
Petamem	Petamem Language Server	www.petamem.com	hybrid
Promt GmbH	PROMT Translation server 8.0; Intranet Edition; PROMT NET Professional 8.0; PROMT Translation ASP	www.promt.de	hybrid
Promt GmbH	Online-Übersetzung	www.online-translator.com	hybrid
SDL International	SDL Enterprise Translation Server; Knowledge Based Translation System	www.sdl.com/de	hybrid
Systran	Business Translator; Premium Translator; Enterprise Server 6 etc.	www.systran.de	regelbasiert

Zweck tauscht Linguatec Daten mit professionellen Translation Memories aus, zum Beispiel mit einem führenden System Trados von SDL International.

Eine Verbindung der beiden methodischen Ansätze strebt Euromatrix (www.euromatrix.net) ebenso an. Mit dem Projekt will die EU die Bedürfnisse der europäischen Mitglieder unterstützen. Bislang dominieren die USA die Forschung in Bezug auf die englische Sprache. In Europa gelten andere Anforderungen: Zwar übersetzt das europäische Parlament seine offiziellen Papiere derzeit in elf Sprachen, die übrigen 12 Amtssprachen gehen aber leer aus.

Die EU nutzt das regelbasiert arbeitende System von Systran und verspricht sich nun eine schnellere Integration weiterer Sprachpaare. Das schaffen statistische Methoden – geeignete Paralleltexte vorausgesetzt – eher, da sie keine Grammatik benötigen. Entwickelt haben die Forscher einen statistischen Decoder namens Moses (www.statmt.org/moses), eine Open-Source-Werkzeugsammlung, die das Training neuer Kombinationen unterstützt, indem sie zueinander passende Wortgruppen aus Paralleltexten einander gegenüberstellt (Alignment) und eine Phrasentabelle erzeugt. Mit solchen Tabellen und statistischer Übersetzung arbeitet auch Google, das mit seinem System tiefen Eindruck in der Übersetzungsszene hinterlassen hat.

Viele Forschungsgruppen und Hersteller nutzen Moses als Grundlage, war aus Saarbrücken zu erfahren. Dort sitzen die Koordinatoren des Projekts um den Saarbrücker Computerlinguistik-Professor Prof. Hans Uszkoreit. Projektpartner sind die Edinburgh University, die Charles University, CELCT (www.celct.it), Morphologic (www.morphologic.hu) und die Group Technologies AG (www.group-technologies.com).

Verbesserungen durch Benutzer-Feedback

Mittelfristig soll eine Architektur entstehen, die beide Ansätze berücksichtigt. Hierfür übersetzen die Wissenschaftler Texte mit existierenden Produkten und vergleichen die oft unterschiedlichen Ergebnisse, um das Beste aus den Systemen herauszuholen. Hersteller können daraus wertvolle Erkenntnisse gewinnen. Im Nachfolgeprojekt Euromatrix, das im Februar 2009 ausläuft, wollen die Projektbeteiligten das Feedback der Nutzer zu den Übersetzungen gleichzeitig zur Verbesserung der Systeme verwenden, womit Google seit Längerem Erfolg hat.

Wer ein maschinelles Übersetzungsprogramm in seinem Unternehmen einsetzen möchte, sollte nicht denken, dass es „out of the box“ spontan zufriedenstellende Ergebnisse liefert – eine Erwartungshaltung, die bei vielen potenziellen Kunden existiert. Eine funktionierende Anwendung entsteht nur durch eine Integration in die Unternehmensanwendungen. Das betonten meh-

Fallen maschineller Übersetzung

Wer den Satz

Mutter a bitte fest anziehen

ins Englische übersetzt, erhält:

a: *Mother a please firmly draw*

b: *Please make sure a mother attract*

c: *A mother ask tighten*

Zurückübersetzt kommt heraus:

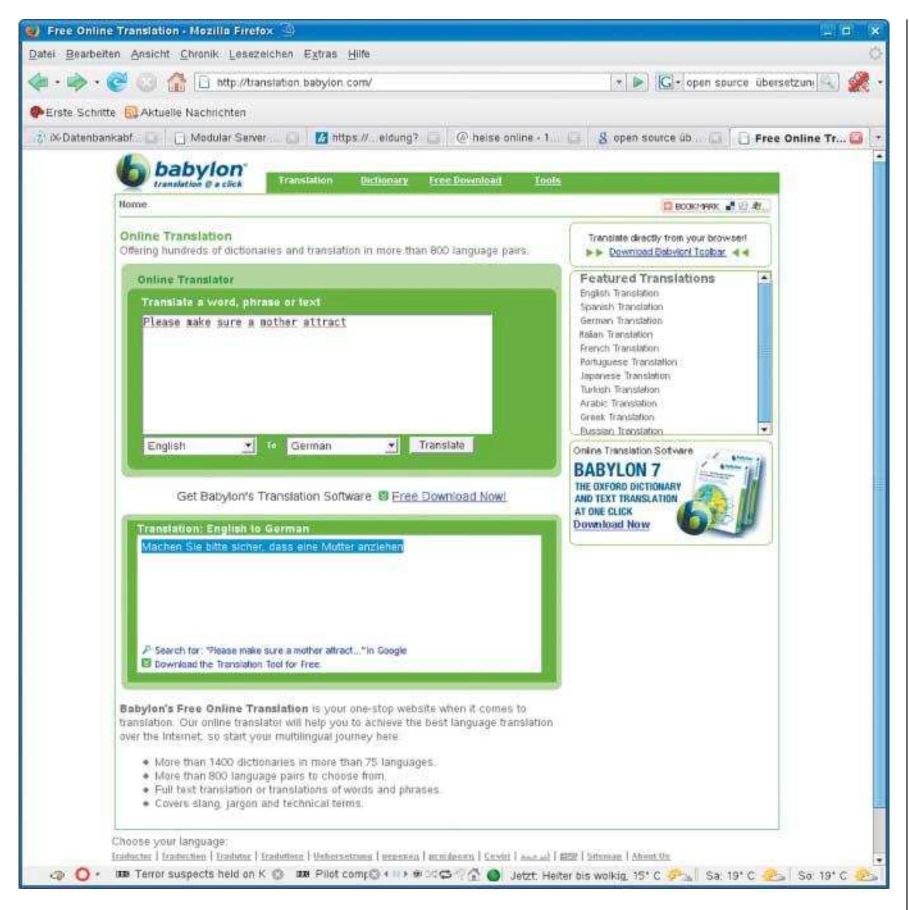
a: *Bemuttern Sie bitte fest Attraktion*

b: *Machen Sie bitte sicher, dass eine Mutter anziehen*

c: *Eine Mutter fragen verschärfen*

Maschinelle Übersetzer kommen ohne eine Überprüfung durch Sprachkundige noch nicht aus.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Freiraum: Baylon rechnet wohl mit längeren Texten, jedenfalls lädt das Eingabefeld dazu ein (Abb. 2).

Anzeige

rere Hersteller bei der telefonischen Recherche, zum Beispiel Lucy Software and Services. Dort hält man die Einbettung in das Unternehmensumfeld für eine der größten Herausforderungen, wichtiger noch als die Übersetzungsalgorithmen. Viele Kunden aus großen internationalen Konzernen fragen vor allem nach einer SAP-Integration. Im Einsatz ist der Lucy Translator, dessen Endbenutzerversion Langenscheidt als T1 verkauft, unter anderem bei SAP im Helpdesk. Denn nachts bearbeiten die Kollegen aus Indien die Tickets.

Fazit

Systematischer Aufbau und Verwaltung einer einheitlichen Terminologie, übersetzungsgerechtes Schreiben und die Verwendung standardisierter Begriffe erhöht die Übersetzungsqualität, sodass in eindeutig definierten Fachgebieten mit besseren Ergebnissen zu rechnen ist. Die Erwartungshaltung der Anwender ist hoch. Hersteller und Forscher stehen vor der Aufgabe, die Qualität der angebotenen Übersetzung durch eine Kombination regelbasierter mit statistischen Verfahren zu verbessern, um die Akzeptanz weiter zu erhöhen.

Erreichbar wird dies nicht allein durch eine Verbesserung der Übersetzungstechnik, sondern auch durch praktische Maßnahmen, etwa durch eine Erweiterung der Glossare oder einer weiteren Einbeziehung von Translation Memories. Der Bedarf an maschineller Übersetzungssoftware in Unternehmen und Parlamenten steigt – dank multilingualer Informationsfluten im Internet und der vielbeschworenen Globalisierung. Grundsätzlich gilt die Abhängigkeit der Übersetzungsqualität vom Kontext, jenseits derer dürfte nach wie vor genügend Material anfallen, das zur allgemeinen Erheiterung beitragen wird – vom Zeitalter des Übersetzungsimplantats à la Babelfisch sind alle noch weit entfernt. (rh)

BARBARA LANGE

ist IT-Journalistin und Inhaberin des Redaktionsbüros kurz&einfach in Lengede.





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Netbooks mit Atom-CPU von Acer und Asus

Winzigkeiten

Nikolai Zotow, Ralph Hülsenbusch

Trotz kleiner Bildschirme und Tastaturen mit Gewöhnungsbedarf: Die Winzlinge im 30-Zentimeter-Format erfreuen sich großer Beliebtheit und legen an Leistung zu. Bestechend sind Leichtigkeit und die geringe Größe, fraglich ist die Eignung fürs Geschäftliche.

Mit dem Aspire One hat Acer auf die überraschend erfolgreiche Markteinführung des Asus Eee PC reagiert. Nachdem die Kategorie des Netbooks anfangs nur für Surfen und E-Mail unterwegs mit gelegentlichen kleineren Office-Aufgaben gedacht war [1], mausert sich Acers Aspire One zum fast vollwertigen kleinen Subnotebook, und Asus zieht mit seinem Eee PC 900a nach. Beide nutzen Intels jüngsten Spross fürs Mobile, Näheres dazu im Textkasten „Intels Atom-Prozessor“.



Acers Aspire One 150X

In der Version 150X verfügt das Aspire One über eine 2,5-Zoll-Festplatte mit 120 GByte und 1 GByte Arbeitsspeicher. Er besteht aus zwei 512 MByte großen DDR2-SDRAM-Modulen, von denen eins fest auf der Mutterplatine verlötet ist. Der Speicher sitzt unter der Hauptplatine, was die vollständige Zerlegung des Netbooks erfordert.

Das 150X wird, wie das „X“ in der Modellbezeichnung andeutet, mit Windows XP ausgeliefert. Die Installationsdateien des Betriebssystems befinden sich auf einer versteckten Partition der Festplatte. Laut offiziellen Angaben ist der Rechner für Vista zu klein dimensioniert. Im Test versah das Aspire One dennoch unter Microsoft Windows Vista Ultimate seinen Dienst.

Der mitgelieferte Drei-Zellen-Akku mit 2200 mAh hält knapp zwei Stunden durch. Empfehlenswert die zusätzliche Anschaffung eines mit 2600 mAh und sechs Zellen für 99 Euro. Im Testbetrieb, der mit eingeschaltetem WLAN und abgeschalteten Schlafmodi im „Battery Eater“ (www.batteryeater.com) eine Dauernutzung simuliert, hielt eine Ladung mit dem mitgelieferten Drei-Zellen-Akku maximal 120 Minuten.

Zwar kleiner als üblich, für gelegentliches Tippen aber ausreichend ist das Keyboard. Beim Mauspad befinden sich die Tasten nicht wie gewohnt unter der Sensorzone, sondern daneben. Das erschwert ein Drag & Drop mit einer Hand. Der Notebookdeckel besitzt keine Verriegelung, er schließt über einen Federzug. Man muss mit beiden Händen zugreifen, um das Notebook zu öffnen, was zu unschönen Fingerabdrücken auf dem Display-Rand führt.

Wenig Klangfreude wecken die blechern klingenden eingebauten Lautsprecher. Dafür hat das Aspire One mit einem integrierten Mikrofon und einer eingebauten Webcam mit 0,3 Megapixeln Auflösung alles für die Webkonferenz an Bord.

Neben WLAN geht es über Ethernet ins LAN. Positiv fällt der kleine Schiebeschalter an der Vorderseite zum Abschalten des drahtlosen Netzes auf. Acers Netbook besitzt zwei Card Reader: Einer dient unter Linux als Erweiterung des SSD-Plattenbereiches, unter Windows fungiert er als weiteres logisches Laufwerk, ausschließlich mit SD-Karten. Der andere Multi-Card-Reader eignet sich darüber hinaus für alle anderen Varianten.

Acer hat das Aspire One für Privatanwender konzipiert. Nicht zuletzt das spiegelnde Display und der glänzende Schäuble-Kollektor, die Fingerabdrucksammelfläche auf dem Notebookdeckel, schränken den Einsatz im harten Alltagsgeschäft ein. Der Bildschirm wäre hell genug für die Nutzung unter freiem Himmel sowie in hellen Räumen. Leider macht das „Crystal Brite“-Display den Vorteil zunichte. Von der Leistung her reichen die Ressourcen durchaus für den mobilen professionellen Einsatz, wie die Experimente mit den üblichen Büroanwendungen unter Vista gezeigt haben. Acer will das Aspire One 150X ab Mitte Oktober mit einer 160 GByte großen Festplatte ausliefern.

Daten und Preise

Netbooks

Identische Hardware: Atom N270, 1,6 GHz, 24 KByte L1-, 512 KByte L2-Cache, 533 MHz Frontside-Bus; Chipset „Poulsbo“ (945GSE mit 82945GBM); kein Bluetooth; 10/100-MBit-Ethernet, drei USB; Kopfhörer- und Mikrofonanschluss, 0,3-Megapixel-Webcam mit Mikro; VGA

Acer Aspire One 150X

Hardware: SATA Festplatte, 2,5 Zoll, 120 GByte; 1 GByte RAM (2 × 512 GByte, ein Modul nicht wechselbar); zwei SD-Slots

Hersteller: Acer, www.acer.de

Preis: 389 Euro (brutto)

Asus Eee PC 900A

Hardware: SDD-Modul, 8 GByte; 1 GByte RAM (1 Slot); SD-Slot

Hersteller: Asus, www.asus.de

Preis: 278 Euro (brutto)

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Eingeschränkt: Bei Acers Aspire One ist der eine Speicherbaustein fest verdrahtet, wechseln lässt sich nur der zweite.

Entgegen dem ersten Anschein (Abbildung) lässt sich das 150X nicht nachträglich mit einem UMTS-Modul ausrüsten. Der freie Slot ist zwar vorhanden, es fehlt aber die integrierte Antenne.

Asus Eee PC 900A

Beim Eee PC hat Asus UMTS/GPRS bis dato nicht vorgesehen. Der Hersteller schickte das Modell 900A auf Wunsch mit Xandros-Linux basierend auf dem Kernel 2.6.21.4-eeepc.

Asus' 900A verfügt über 1 GByte DDR2-RAM und eine 8 GByte große Solid State Disk (SSD), zur Hälfte belegt. Der Bildschirm hat mit 8,9 Zoll dieselbe Größe wie beim Aspire One. Hauptsächliche Unterschiede zum Aspire One stecken im Detail. Der Eee PC ist völlig geräuschlos, verbraucht weniger Strom und erlaubt ein längeres Arbeiten mit einer Akkuladung, dank SSD. Asus spricht von vier Stunden unter Linux bei abgeschalteten WLAN, Bluetooth und Kamera. Der Bildschirm ist nicht verspiegelt, sodass ein heller Hintergrund die Lesbarkeit kaum beeinträchtigt.

Kompaktheit hat ihren Preis: Der Eee PC 900A besitzt fast die gleichen Maße wie der erste Eee PC 4G [1] und ist 2,5 cm schmaler als das Aspire One, was zu noch kleinerer Tastatur führt. Das Mauspad hat sein Tastenfeld am unteren Ende, es besteht aus einem Stück und funktioniert wie eine Wippe. Nicht sofort erkennt man auf der Tastatur, dass einige Sonderzeichen wie Pipe, Größer- und Kleiner-Zeichen sowie die Funktionen für seitenweises Blättern nur über die blaue Funktionstaste „FN“ erreichbar sind. Als Schalter zum geschwinden Kappen der drahtlosen Verbindungen dient FN+F2.

Unter der im Boden befindlichen Platte erreicht man nach Lösen der beiden Schrauben die SSD und den Speicherriegel, für den es nur einen Steckplatz gibt. Die Ausstattung mit Schnittstellen ist nahezu identisch mit der des Aspire One, nur der zweite SD-Slot fehlt. Und wie das Gerät von Acer verfügt auch der Eee PC 900A über eine eingebaute 0,3-Megapixel-Kamera nebst Mikrofon. Am Markt ist es ab 278 Euro zu haben.

Intels Atom-Prozessor

Der jüngste Spross für Eingebettete aus Intels Chipschmiede, der Atom namens Diamondville, besitzt zwei Ableger für PCs: den N270 für Netbooks und den 230 für „Nettops“, die sparsamen Desktop-Rechner. Den Atom-Prozessor produziert Intel in 45-Nanometer-Technik. Von der Sockelgröße her zählt er zu den kleinsten x86ern. Beide Varianten laufen mit 1,6 GHz, haben einen 533 MHz schnellen Frontside-Bus, 24 KByte L1- und 512 KByte L2-Cache. Der Chipset „Poulsbo“ vereint den 945GSE und 82945GBM für die Grafik in einem Baustein. Der Atom kommt mit einer Leistung von 0,6 bis 2,5 Watt aus – ein Zehntel des in Subnotebooks verbreiteten Centrino M. Atom und Poulsbo bilden die Menlow-Plattform, die Intel als Centrino Atom vermarktet. Wieder aufgenommen hat Intel beim Atom das Hyper-Threading (HT), sodass aus Sicht des Betriebssystems zwei logische CPUs zur Verfügung stehen – nicht zu verwechseln mit der Dual-Core-Technik. Asus nutzt bei seinem Eee PC die HT-Option jedoch nicht.

Fazit

Innerhalb des letzten halben Jahres haben die Netbooks von der technischen Entwicklung profitiert. Ein Gigabyte Hauptspeicher gehören zur üblichen Ausstattung, nur beim Massenspeicher scheiden sich die Geister. Für eine normale Harddisk spricht, dass sie viel Speicher für wenig Geld bereitstellt, dafür aber mehr Strom verbraucht als die vergleichsweise teuren SSDs. Außerdem sind mechanische Laufwerke stoßempfindlicher als rein elektronische SSDs. Abgesehen davon, dass Harddisk nicht geräuschlos sind und zusätzlich Wärme abgeben, was eine entsprechende Kühlung erfordert.

Ob er Windows oder Linux auf den Minis den Vorzug geben möchte, kann der Kunde selbst entscheiden. XP braucht mehr Speicher, fügt sich aber in der Regel reibungsloser in die betriebliche Umgebung ein. Linux kommt samt einer kompletten Büroumgebung nebst einiger Werkzeuge mit 4 GByte auf dem Speichermedium aus, solange es sinnvoll eingerichtet wurde. Wer aber den Verlockungen weiter Add-ons erliegt, gar eine komplette Entwicklungsumgebung nutzen möchte, stößt bei SSDs schnell an Grenzen.

Mit beiden Netbooks lassen sich die üblichen Tätigkeiten, die man unterwegs mit einem Notebook durchführen möchte, erledigen – zur Entspannung kann man auch mal Musik hören oder einen Film anschauen, allerdings nur von einem USB-Medium oder einer Memory-Card. (rh)

iX-Wertung

Acer Aspire One 150X

⊕ zweiter SD-Slot
⊕ 120-GByte-Festplatte (SATA)
⊕ Hyper-Threading aktivierbar

⊖ Speicher nur schwer zu erweitern
⊖ Festplatte nicht wechselbar
⊖ kein UMTS/GPRS
⊖ kein Bluetooth

Asus Eee PC 900A

⊕ lange Akkulaufzeit
⊕ geräuschlos
⊕ SSD und Speicher zugänglich

⊖ kleiner Massenspeicher
⊖ kleine Tasten
⊖ kein Hyper-Threading
⊖ kein Bluetooth

Literatur

[1] Martin Schmitz; Mini-Notebook; Leicht befunden; Berufliche Eignung des Low-Cost Eee PC 4G von Asus; *iX* 4/2008, S. 87

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Acers Notebook mit AMDs Turion: Travelmate 5530

Schwungvoll

Ralph Hülsenbusch

Als Notebook für Profis mit hoher Performance bewirbt Acer sein Notebook Travelmate 5530, bietet es aber seinem gesamten Kundenkreis an. Vom Preis her liegt es auf dem Niveau handelsüblicher Laptops.

Zum Test schickte Acer ein Travelmate 5530G 703G25Mi mit AMDs RM-70-CPU, die 2 GHz schnell und deren L2-Cache 1 MByte groß ist. Das professionelle Notebook taucht in drei Untervarianten auf: als 702, 703 und 823. Der Unterschied liegt in der Ausstattung. Acer bietet es mit 2 und 3 GByte von Haus aus an. Der 823er arbeitet mit dem ZM-82-Prozessor von AMD, der mit 2,2 GHz läuft und einen 2 MByte großen L2-Cache besitzt.

Acers Travelmate 5530G betreibt eine ATI HD 3200 und eine HD 3470 X2 zusammen als sogenannte Hybrid Crossfire. Das heißt, beide Prozessoren arbeiten im Wechsel, was die Leistung in die Nähe einer High-End-Grafik bringen soll. Das Ergebnis bleibt aber weit darunter. Man mag einwenden, dass das für Profi-Notebooks unwichtig sei, aber die Zahl der grafiklastigen Anwendungen wächst. Ab der Treiberversion 8.8 soll auch XP Hybrid-Crossfire unterstützen, installiert war 8.479.1.0. Im 3DMark und bleibt die Kombination mit 1671 im unteren Drittel.

Für den professionellen Einsatz bestechender ist die Ausstattung mit 3 GByte DDR2-RAM, die sich auf 4 GByte erweitern lassen, und die 250 GByte große SATA-Platte. Das hat allerdings seinen Preis. Im Dauerbetrieb mit aktiviertem WLAN reicht die Akku-Ladung für höchstens 1,5 Stunden. WLAN und Bluetooth besitzen separate Schalter, lassen sich also ad-hoc stilllegen und sind nach wenigen Minuten wieder aktiv – eine ratsame Spar- und Sicherheitsmaßnahme. Es fehlt ein UMTS/GPRS-Modul, was die Freiheit erheblich einschränkt – schlimmer noch, es ist nicht vorgesehen. Bleibt also nur der Ausweg über USB oder PC-Karten. Innovativ sind HDMI und eSATA.

Zu den Geschmacksachen zählt die leicht geschwungene Tastatur, die wohl die Handgelenke etwas entlasten soll. Im Test ließ sich gut damit arbeiten, einzig bei den am linken Rand angebrachten Sondertasten kam es gelegentlich zu Missgriffen. Ebenso exotisch ist die Lage der Währungssymbole für Euro und US-$ im Cursorblock.

Konzessionen an neue Medien in der Kommunikation sind das integrierte Stereomikrofon und die im Bildschirmrahmen eingebaute Kamera. Andererseits hat Acer besonderen Wert auf Sicherheit gelegt und einen Fingerabdruckleser zwischen die beiden Maustasten gebaut. Dazu installiert der Hersteller sein Softwarepaket Bio Protection ab Werk. Es verlangt allerdings die komplette Verriegelung von BIOS und Harddisk mit Passwörtern. Als weitere Pakete liegen Acers Crystal Eye View für die Webcam, Empowering Technologie und Grid View bei. Bei Letzterem handelt es sich um die Option, mehrere Desktops darstellen zu können.

Zu guter Letzt kann Acers Travelmate bei der Verarbeitung punkten: mit straffer Mechanik, übersichtlicher Beschriftung sämtlicher Schnittstellen seitlich der Tastatur und vor allem mit dem gut erreichbaren Zugang zu Speicher, Festplatte sowie WLAN-Modul. Zwar sind ein paar Schrauben mehr zu lösen, dafür kommt man an die Module gut heran und erreicht zugleich den Lüfter. Das kann hilfreich beim Entfernen unliebsamer Staubmäuse sein, die manch anderem Laptop schon den Garaus gemacht haben.

Fazit

Travelmate 5530G ist das erste Notebook von Acer mit AMDs Mobileprozessor Turion, Codename Puma. Der Hersteller bietet es allen Kunden an, was den technischen Gegebenheiten nicht in jedem Fall entspricht. Für das Home Entertainment fehlt es an Leistung bei der Grafik, für die Mobilität UMTS/GPRS. Dafür gibt es Optionen wie PC-Card und HDMI, die ein Argument sein könnten, sich für das solide Gerät zu entscheiden. (rh)

Daten und Preise

Travelmate 5530 703G25Mi

Hardware: AMDs Turion X2 RM-70, 2 GHz, 24/24 KByte L1-, 1 MByte L2-Cache; 3 GByte RAM (ein 1024-MByte-, ein 2048-MByte-Modul DDR2-RAM); ATI HD 3200 (on board), HD 3470 X2 (256 MByte); 15,4 " WXGA; 250 GByte SATA; DVD (DL); Fingerabdrucksensor; Klinkenbuchse für Audio-in, -out und Mikrofon, Stereo-Mikro und -Lautsprecher eingebaut; Webcam; Broadcom Netxtreme Gigabit Ethernet (auf 10/100 MBit limitiert) 4 × USB; HDMI; eSATA; VGA; Modem; Docking-Anschluss

Software: Crystal Eye View; Empowering Technology; Bio Protection; Grid Vista

Hersteller: Acer, www.acer.de

Preis: 671,43 Euro

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

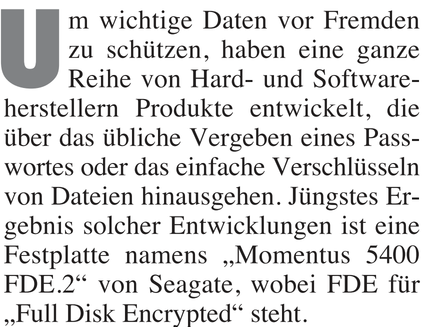
Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Laptop von Dell mit geschützter Platte

Schlossendlich

Ralph Hülsenbusch, Volker Tanger

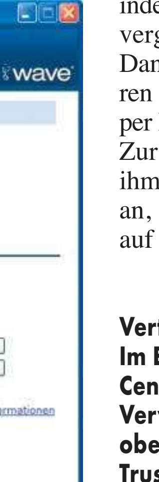


Das Notebook ist weg – ärgerlich zwar, aber an die Daten kommt sowieso niemand heran, denn schließlich handelt es sich ja um das Latitude D630 mit der hardwaregestützten Verschlüsselungtechnik von Seagate – da kann eigentlich nichts passieren.

Um wichtige Daten vor Fremden zu schützen, haben eine ganze Reihe von Hard- und Softwareherstellern Produkte entwickelt, die über das übliche Vergeben eines Passwortes oder das einfache Verschlüsseln von Dateien hinausgehen. Jüngstes Ergebnis solcher Entwicklungen ist eine Festplatte namens „Momentus 5400 FDE.2“ von Seagate, wobei FDE für „Full Disk Encrypted“ steht.

Sämtliche Daten auf dem Speichermedium zu verschlüsseln bringt Vorteile: Der Anwender braucht sich nicht um spezielle Daten zu kümmern wie ausgelagerte Speicherbereiche, Caches, Konfigurationsdateien oder Anwendungskonfigurationen, sie bleiben für Nichtautorisierte verborgen. Dem stehen gegenüber: Die permanente Verschlüsselung geht zu Lasten des Datendurchsatzes, bei Notebooks muss man auf den Schlafzustand verzichten, da das Betriebssystem beim Neustart auf verschlüsselte Daten trifft, und zentrale Updates sowie Patches können für stationäre Systeme nur im aktivierten Zustand funktionieren.

Dell liefert zum Test sein Latitude D630 mit Seagates ST980816AS (80 GByte, 5400 UpM); der Zugriffsschutz war deaktiviert. Der Eigentümer muss zuerst in der mitgelieferten Sicherheitssoftware von Wave (www.wave.com), dem Embassy Security Center, den „Trusted Drive Manager“ (TDM) finden und aufrufen. Nachdem das Programm das FDE-Laufwerk lokalisiert hat, kann er es „initialisieren“, indem er ein Passwort vergibt und bestätigt. Danach darf er weiteren Benutzern Zugang per Passwort erlauben. Zur Sicherheit bietet ihm der TDM noch an, die Informationen auf einem Wechselmedium, etwa einem USB-Stick, zu hinterlegen. Den soll man tunlichst nicht offen herumliegen lassen, da alle Daten wie Seriennummer, Security-ID, Benutzernamen und Domain in einer XML-Datei im Klartext gespeichert sind, selbst das Passwort. Der Hersteller argumentiert, dass dies beabsichtigt sei. Es handle sich um ein Grundprinzip von IT-Sicherheit: Am Ende der Sicherungskette müssten die Daten im Klartext zugänglich sein. Wären diese immer noch verschlüsselt, bestünde die Gefahr das man nicht mehr an die Daten komme. Selbstverständlich gehöre das USB-Drive eingeschlossen. Man habe diese Methode als die für den Einzelnutzer wohl am praktischste ausgewählt, da solche Medien überall verfügbar sind.



Vertrauenssache: Im Embassy Security Center gibt es die Verwaltungsoberfläche für das Trusted Drive – hier ist der Schutz lokal eingerichtet.

Für zentrale Administration konzipiert

In der Regel dürfte aber die Alternative für Firmen der bessere Weg sein: Der Admin des Hauses kann sämtliche FDE-Notebooks, die im Netz sind, zentral mit je einem Passwort versehen und auf einem Server verwalten. Dazu muss dort der TDM remote installiert sein, was Kosten in Höhe von rund 1400 Euro für 20 Benutzer verursacht.

Auf dem Notebook war in einer virtuellen Umgebung unter VMwares Player der Windows Server 2003 nebst TDM installiert, sodass man im Virtuellen die Rolle des Administrators spielen konnte. Zusätzlich lag eine Datei auf

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

dem Desktop, die eine genaue Anleitung für das Experiment enthielt – es funktioniert ohne langwierige Einarbeitung.

Nimmt man die Technik genauer unter die Lupe, erkennt man einen maßgeblichen Unterschied zu anderen Verschlüsselungsmethoden: Der Controller der Momentus FDE von Seagate verschlüsselt immer. Der Passwortschutz steuert das Entschlüsseln, indem er ohne Vergabe die Daten für jeden bereitstellt, beim Aktivieren des Schutzes jedoch nur noch für die autorisierten Benutzer. Im Test bewies ein Plattenperformance-Test, dass es zwischen geschützter und nicht geschützter Platte keinen Unterschied im Durchsatz gibt. Die Messungen mit dem Bonnie lieferten bis auf die Nachkommastellen genau dieselben Resultate.

Danach fanden weitere Experimente statt, unter anderem der Versuch, das geschützte Laufwerk in einem anderen Notebook zu verwenden. Wie zu erwarten, ist ein Zugriff auf die Daten nicht möglich, der Rechner findet keine bootfähige Platte. Per USB über einen externen Anschluss an einem PC betrieben, erscheint die 80 GByte große Momentus 5400 FDE mit einem 128 MByte großen unformatierten Bereich, der Rest bleibt unsichtbar. Nach dem Entriegeln hat man eine „normale“ Harddisk mit Filesystemen vor sich, in diesem Fall NTFS.

Allein das Passwort schützt

Laut Aussage von Seagate nutzt die Passwortvergabe dieselbe Technik wie der Passwortschutz im BIOS für Festplatten im ATA-Modus. Prinzipiell kann der Anwender mit dem geschützten Laufwerk von einem Notebook zu einem anderen wechseln – etwa bei einer Neuanschaffung. Doch sogar bei demselben Hersteller ist nicht garantiert, dass das BIOS respektive der Controller das Passwort richtig erkennt. Die Hersteller weichen in ihren Regeln für gültige Passwörter voneinander ab. Außerdem hat jeder seine eigene Methode, das Passwort auf die Länge von 128 Bit (AES) aufzufüllen. Es gibt allerdings Bestrebungen, im ATA-Standard für eine Vereinheitlichung zu sorgen. Dell jedenfalls sichert zu, dass man die FDE-Platte weiterverwenden kann.

Datenschutz per FDE-Platte zu genießen erfordert zuverlässige und ebenso gut geschützte Sicherungsverfahren, denn kommt es zum Malheur, etwa durch einen technischen Defekt oder Verlust des Notebooks, sind die Daten unwiederbringlich verloren. Wer ein FDE-Notebook klaut, kommt an die gespeicherten Informationen nicht heran, da er in der Passwortabfrage hängen bleibt und den Rechner nicht hochfahren kann. Mit einer Live-CD kann er bestenfalls auf das Entschlüsselungstool in der Minipartition zugreifen.

Fazit

Notebooks mit FDE-Platten und einer zentralen Verwaltung bieten einige Vorteile: Sie sind geschützt und der Nutzer braucht nur seine Zugangsdaten zu kennen. Dell bietet auch andere Latitude-Modelle mit verschlüsselten Laufwerken an.

Bei FDE-Platten entfällt das zeitaufwendige sichere Löschen der Daten durch mehrfaches Überschreiben, wie es der US-amerikanische Standard NISPOM (US DoD 5220.22-M) und die Richtlinie zum Geheimschutz von Verschlusssachen beim Einsatz von Informationstechnik des Bundesamtes für Sicherheit in der Informationstechnik vorschreiben. Das kann bei heute üblichen Festplatten mit mehreren 100 GByte bis zu einer Woche dauern. Deshalb arbeitet Seagate inzwischen an einem Verfahren, die Technik auf Massenspeicher von Servern anzupassen. (rh)

VOLKER TANGER

ist Security Consultant bei der HiSolutions AG in Berlin.





Laborbericht extern

Bei den Versuchen, der Verschlüsselung auf den Zahn zu fühlen und eventuelle Sicherheitslücken zu finden, traten folgende Dinge zutage:

Solange die Festplatte noch mit Strom versorgt wird, bleibt die Freischaltung erhalten. Wäre es möglich, einen Warmstart auszulösen, könnte ein Angreifer etwa mit einer Linux-CD/DVD immer noch auf die ungeschützte Platte zugreifen. Hibernate-to-Disk, hartes Stromabschalten, Reboot und ähnliche Methoden setzen die Platte auf „verriegelt“ zurück.

In diesem Fall erscheint das Laufwerk ohne Partitionstabelle mit einer Größe von 134 MByte beim 120-GByte-Modell und 128 MByte bei dem mit 80 GByte. Auf der Mini-„Platte“ befindet sich ein 21 KByte großer Bootloader (pbMBR v1016), der eine mit dem aus alten DOS-Zeiten bekannten EXE-Packer *PKLITE* komprimierte EXE-Datei startet. Sie lässt sich mit *UNP.EXE* dekomprimieren und enthüllt ein DOS-Programm, das zwar für Bildschirmausgaben und Zeitabfragen BIOS-Interrupts nutzt, für Tastaturabfragen dagegen direkt auf Hardwareregister zugreift. Außerdem nutzt die Software direkt die Register eines PCI-on-board-ATA-Controllers. Das erklärt, warum eine Entriegelung der FDE-Platte über einen USB-Adapter nicht funktioniert.

Als Gegenprobe kam die entpackte EXE-Datei auf eine PC-DOS-Diskette, von der aus der Rechner ein klassisches DOS hochfährt. Ruft man die Datei vom DOS-Prompt auf und gibt Benutzernamen und Passwort ein, beendet sich das Programm. Beim anschließenden Warmstart etwa mit einer Linux-Boot-CD ist die Platte entriegelt.

Untersuchungen mit dem ATA Forensic Toolkit (TAFT) und HDAT2 sowie Linux-Tools ergaben keinen Hinweis, dass der Controller einfach die Host Protected Area (HPA) oder ein Device Configuration Overlay (DCO) nutzt. Allerdings scheint er sowohl im verriegelten als auch im offenen Zustand auf eine ganze Reihe von ATA-Kommandos fehlerhaft zu reagieren, er unterstützt zum Beispiel kein SMART-Monitoring.

iX-Wertung

⊕ einfache Handhabung
⊕ zentralisierter Schutz für Notebooks
⊖ XML-Datei mit Nutzerdaten nicht verschlüsselt
⊖ nur für Windows XP

Daten und Preise

Latitude D630 FDE

Hardware: Core 2 Duo T7300, 2 GHz; 2,5 GByte RAM; Momentus 5400 FDE.2 von Seagate ST980816AS, 80 GByte; 14,1 Zoll TFT-Display, 1280 × 800

Software: Dell Wave Embassy Security Center

Hersteller/Anbieter: Dell, www.dell.de

Preis: D630 FDE 702 € (Teststellung, FDE-Disk 27 € Aufpreis), Wave Embassy Remote 1400 € (20 User)

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.







Drei Monitore mit RGB-LED-Backlight

Dreigestirn

Dieter Michel

Langsam, aber sicher erobern LC-Displays mit LED-Hintergrundbeleuchtung die Regionen außerhalb der Druckvorstufe. Erste Vertreter aus Büroumfeld und Videobearbeitung mussten im *iX*-Labor einem Repräsentanten des Preprints gegenübertreten.

Als das Fachpublikum den ersten Computermonitor mit LED-Backlight zunächst noch wie ein exotisches Tier beäugte, waren die potenziellen Vorteile der Technik bereits erkennbar: Die Intensität der Primärfarben Rot, Grün und Blau lässt sich über die Hintergrundbeleuchtung individuell steuern. Statt die Farbtemperatur über das LCD-Panel zu beeinflussen und dabei den Kontrastumfang und die Helligkeitsabstufungen in den einzelnen Farbkanälen zu opfern, kann man die Farbtemperatur sehr genau allein mit dem Backlight einstellen und gegebenenfalls sogar mit Farbsensoren konstant halten.

Da Leuchtdioden ein Licht mit hoher spektraler Reinheit und sehr hoher Farbsättigung erzeugen, lassen sich mit ihnen Monitore mit großem Farbraum bauen. Inzwischen gibt es LED-Backlights aber nicht nur bei Profi-Monitoren für Druckvorstufe und Grafik, vielmehr findet man die LED-Technik bereits in den ersten Büromonitoren. Der Testbericht stellt drei Bildschirme vor, die das gegenwärtig verfügbare Spektrum abdecken – es reicht vom Büromonitor mit erweitertem Farbraum über einen hardwarekalibrierbaren Monitor, der sich besonders für die Druckvorstufe eignet, bis hin zu einem Multitalent mit wählbaren Farbräumen sowie analogen und digitalen Videoeingängen und Bild-im-Bild- oder Picture-in-Picture-Funktionen (PiP).

Das breite Display-Format, das alle drei getesteten Monitore aufweisen, bietet eine Auflösung von 1920 × 1200 Bildpunkten, ermöglicht also ohne Interpolation eine verlustfreie Darstellung des vollen High-Definition-Formats von 1920 × 1080 Bildpunkten. Mit einem Seitenverhältnis von 16:10 ist die Bildhöhe (um 120 Zeilen) etwas größer als bei HD, dadurch passt zum Beispiel bei der Videobearbeitung die Timeline unter die Filmvorschau. Anwendern im Print-Bereich kommt das Format insofern entgegen, als es die Darstellung auch einer Doppelseite in guter Auflösung erlaubt und dabei am seitlichen Rand noch Platz bleibt für Werkzeugpaletten und sonstige Bedienfunktionen, etwa eines Layout-Programms.

Der Preis der Anwendung

Beim Thema Print- und Videoproduktion kommt – wenn es um Monitore mit professionellem Anspruch geht – auch gleich die Frage der Farbwiedergabe ins Spiel. Beim Layout von Print-Produkten am Bildschirm möchte man gleich sehen, wie das Endprodukt aussieht („what you see is what you get“) – Ähnliches gilt für die Videobearbeitung. Bei hohen Ansprüchen an die Farbtreue der Bildschirmdarstellung kommt man normalerweise um eine Farbkalibrierung mit passender Soft-

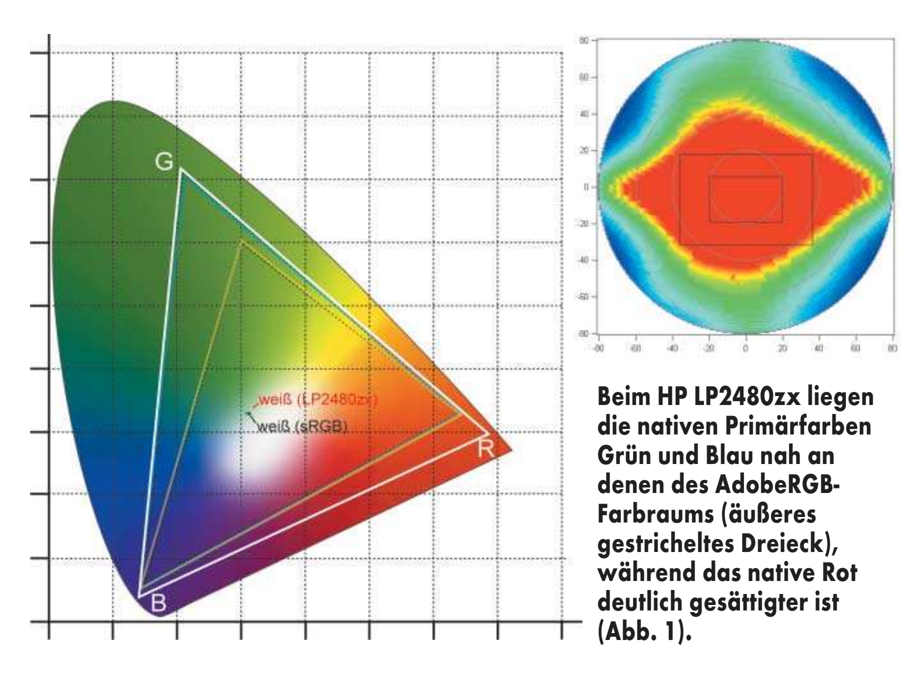
iX-TRACT

- LCD-Monitore mit einer Hintergrundbeleuchtung aus RGB-LEDs können mit einer hohen Farbsättigung der Primärfarben und einem demzufolge großen Farbraum aufwarten.
- Der große Farbraum (Gamut) erlaubt die Emulation verschiedener Standardfarbräume und oft auch die Wiedergabe des vollen Offsetdruck-Farbraums.
- Bei der (Hardware-)Kalibrierung lässt sich der Weißpunkt allein mit dem LED-Backlight einstellen, was mehr Reserven für detailgetreue Helligkeits- und Farbabstufungen lässt.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

ware und einem tauglichen Farbsensor nicht herum.

Hier unterscheiden sich die drei Testkandidaten sowohl im Anspruch als auch im Preis: Der Viewsonic VLED221wm ist ein professioneller Büromonitor für unter 400 Euro netto, der Samsung XL24 ein hardwarekalibrierbarer Monitor, der speziell für die Bildbearbeitung konzipiert wurde und mit 1680 Euro viermal so teuer ist, dafür aber mit passender Kalibriersoftware sowie dem Farbsensor Xrite (ehemals Gretag Macbeth) Display 2 ausgestattet. Der HP Dreamcolor LP2480zx schließlich ist ein Multitalent auf hohem Niveau, das neben einem großen nativen Farbraum und zahlreichen Farbraumemulationen nach internationalen Standards mehrere Optionen der Videowiedergabe sowie die Farbkalibrierung bietet. Auch HDMI und eine Displayport-Buchse fehlen nicht. Dafür liegt der LP2480zx mit einem Netto-Listenpreis von 2299 Euro deutlich über dem Samsung XL24.



Beim HP LP2480zx liegen die nativen Primärfarben Grün und Blau nah an denen des AdobeRGB-Farbraums (äußeres gestricheltes Dreieck), während das native Rot deutlich gesättigter ist (Abb. 1).

HP Dreamcolor LP2480zx



Der HP Dreamcolor LP2480zx ist im Testumfeld zwar der teuerste Monitor, dafür aber auch mit dem größten Funktionsumfang ausgestattet. Das Gehäuse, in mattem Schwarz gehalten, lenkt nicht vom Bildschirminhalt ab. Der Standfuß nimmt wenig Platz auf dem Schreibtisch ein, hinterlässt trotzdem einen soliden und stabilen Eindruck. Der Bildschirm ist ins Hochformat drehbar (Pivot-Funktion).

Fast übersehen könnte man im Normalbetrieb die sechs in den Bildschirmrand integrierten Tasten. Erst das Antippen einer Taste aktiviert deren grüne LED-Beleuchtung und blendet im angrenzenden Bildschirmbereich die gerade aktivierten Funktionen, die sich abhängig vom Kontext des jeweiligen Menüs ändern kann. Bei der Arbeit mit dem Monitor erweist sich dieses Bedienkonzept als ausgesprochen komfortabel – man findet sich sofort in der logischen und übersichtlichen Menüstruktur zurecht.

Mit Anschlüssen hat HP beim LP2480zx nicht gegeizt. Die zwei mittlerweile üblichen DVI-I-Ports, die eine Einspeisung sowohl digitaler als auch analoger RGB-Computersignale erlauben, hat der Hersteller ergänzt durch einen HDMI- und einen Displayport. Den Displayport findet man als Konkurrenzstandard zu HDMI bisher vorwiegend bei Grafikkarten. Obwohl nicht kompatibel zu HDMI, gibt es bereits Grafikkarten mit Displayport, die erkennen können, ob am Ausgang ein HDMI-Adapter steckt, und die Daten dann im korrekten Format senden.

Da der LP2480zx beide Digitalstandards unterstützt, ist er für künftige Entwicklungen gerüstet. Über die bisher erwähnten analogen und digitalen DVI-Schnittstellen hinaus bietet der HP LP2480zx Anschlüsse für Videosignale in den üblichen Formaten Composite Video, S-Video (Y/C) und YUV (Farbdifferenzsignal, Komponentensignal, YPrPb). Daran dürften sich die meisten Videozuspieler anschließen lassen. Hinzu kommt ein USB-Hub mit einem Upstream- und vier Downstream-Anschlüssen, die seitlich rechts am Monitor gut zugänglich sind.

Bei nur einer Signalquelle schaltet der Monitor automatisch auf den gerade benutzten Eingang. Sind Computer- und Videoquellen gemischt angeschlossen, bietet er außer der manuellen Auswahl die Möglichkeit, eine Videoquelle in einem Fenster definierbarer Größe und Platzierung in das Computerbild einzublenden (PiP), was sich etwa für Präsentationen oder Überwachungen eignet. Der eingebaute Videoprozessor kann auch Computerbild und Video gleichberechtigt nebeneinander und nach Wunsch skaliert darstellen.

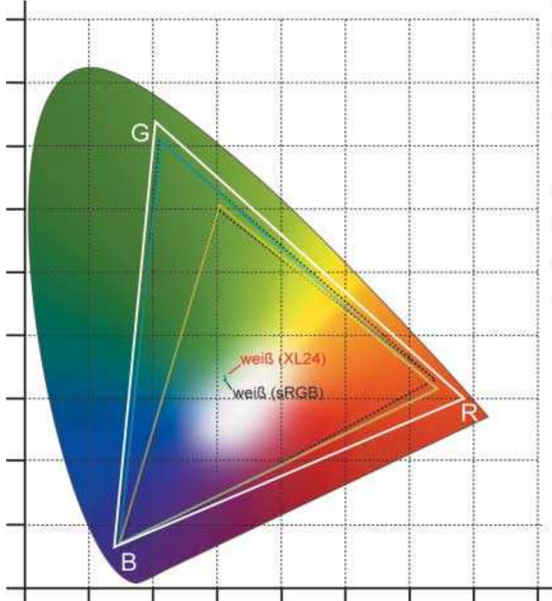
Für Videoschnitt- beziehungsweise -bearbeitungsplätze kann der LCD dank seiner (Digital-)Videofähigkeit in vielen Fällen einen separaten und teuren HD-Vorschaumonitor ersetzen, wobei der HP LP2480zx die nach den entsprechenden Videostandards erforderlichen Farbräume (Rec.601 respektive Rec.709 für HDTV) mit seinem LED-Backlight emulieren kann, sogar den DCI-P3-Farbraum der Digital Cinema Initiative (DCI), der die Farbwiedergabe von Kinofilmen nachbilden soll. Die für einen Computerbildschirm ausgesprochen reichhaltige Auswahl entspringt HPs Anliegen, mit dem LP2480zx einen Bildschirm speziell für die farbgetreue Erstellung und Bearbeitung von Inhalten für die Medienbranche zur Verfügung zu stellen.

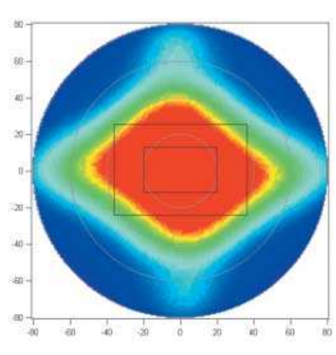
Helligkeit und Kontrast mal richtig

Positiv hervorheben muss man, dass HP auch an die Bezeichnung der Einstellorgane mit professionellem Anspruch herangeht und auf die traditionellen, aber eigentlich falschen Bezeichnungen „Helligkeit“ und „Kontrast“ verzichtet. Nach traditioneller Lesart stellt der Helligkeitsregler den Schwarzpegel und der Kontrastregler die Helligkeit ein. Klingt komisch, ist aber so.

Korrekterweise besitzt ein LCD drei Einstellorgane für das, was das menschliche Auge als Kontrast und Helligkeit wahrnimmt: Schwarzpegel, Gamma und

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.





Der Samsung XL24 zeigt selbst ohne vorherige Kalibrierung eine sehr gute Übereinstimmung der (emulierten) Primärfarben mit AdobeRGB und sRGB. Die nativen Primärfarben, vor allem Rot, sind deutlich stärker gesättigt (Abb. 2).

Helligkeit der Hintergrundbeleuchtung. Genau diese Bezeichnungen verwendet der HP LP2480zx: Der Schwarzpegel stellt ein, wie hell (Leuchtdichte) das dunkelste Schwarz auf dem Monitor sein soll. Eine Veränderung des Gammawertes bewirkt eine Einstellung dessen, was man üblicherweise als Kontrast empfindet. Die Helligkeit der Hintergrundbeleuchtung gibt es nur bei LCDs. Ihre Einstellung hebt oder senkt die Leuchtdichte proportional in allen Bildbereichen, ändert jedoch nicht den Kontrast. Da die Manipulation des Backlights insbesondere nicht die Monitorkalibrierung beeinflusst, ist sie bei kalibrierten Monitoren die einzig – wenn auch nur in Grenzen – erlaubte. Der HP LP2480zx zeigt die Einstellung der Backlight-Helligkeit direkt in der Einheit cd/m^2 an. Auch Anwender ohne entsprechende Messmöglichkeiten können so die empfohlenen Werte für den Betrieb in einer bestimmten Umgebung direkt am Monitor einstellen.

iX-Wertung

HP Dreamcolor LP2480zx

⊕ großer Farbraum

⊕ Emulation von Standard- und User-Farbräumen

⊕ hardwarekalibrierbar

Samsung XL24

⊕ großer Farbraum

⊕ Emulation von Standard- und User-Farbräumen

⊕ hardwarekalibrierbar

⊕ Ausleuchtung kalibrierbar

Viewsonic VLED221wm

⊕ großer Farbraum

⊕ günstiger Preis für einen Monitor mit LED-Backlight

⊖ Farbwiedergabe etwas blickwinkelabhängig

Mit und ohne Treppen

Da HP den Monitor unter anderem für die Videobearbeitung anbietet, musste der LP2480zx mit seiner umfangreicher Ausstattung zusätzlich die ausführliche Prüfung der Qualität der Stand- und Bewegtbildwiedergabe durchlaufen. Als erste Aufgabe musste er die umfangreichen Testpattern der Displaymate Multimedia Edition wiedergeben, sich bei der Bewegtbildwiedergabe speziellen Videosequenzen stellen, die bei SD-Zuspielung (Standard Definition) insbesondere die Qualität von Scaler und Deinterlacer testen. Fazit: Die Entwickler haben sich beim Video-Prozessing für die Bewegtbildwiedergabe nicht lumpen lassen – bei Vollbildwiedergabe ist die Qualität sehr gut und praktisch ohne Artefakte. Im PiP-Betrieb haben sie offenbar etwas weniger Aufwand bei der Interpolation entlang bewegter Kanten betrieben, hier können schon einmal Treppchen sichtbar werden. Bei den Displaymate-Testpattern gibt sich der HP LP2480zx ebenfalls keine Blöße – Auffälligkeiten sind keine zu entdecken.

Durch die für die Hintergrundbeleuchtung verwendeten RGB-Leuchtdioden kann der native Farbraum (Gamut) des HP LP2480zx sehr groß sein, was sich in den Farbmessungen auch bestätigt. Der Monitor emuliert daher Standardfarbräume, die innerhalb seines nativen Gamuts liegen, dadurch, dass er deren Primärfarben als Farbmischungen seiner eigenen, nativen Primärfarben darstellt. Auf dieser Basis gibt er alle anderen (Misch-)Farben so wieder wie ein Monitor mit dem gerade gewählten Standardfarbraum. Dadurch kann die Anwenderin Bild- und Videomaterial in jeweils demjenigen Farbraum bearbeiten, in dem es später wiedergegeben werden soll. Im Farbdiagramm (Abbildung 1) sind der native Farbraum des HP LP2480zx sowie einige emulierte Stadardfarbräume dargestellt.

Damit die Farbraumemulation und die sonstigen Wiedergabeeigenschaften stabil bleiben, bietet HP optional eine Software plus Sensor an, mit deren Hilfe sich der HP LP2480zx kalibrieren lässt. Die Korrekturen, die sich aus einer Kalibriermessung ergeben, werden über USB im Monitor gespeichert. Das Gerät erinnert den Benutzer dann nach einer entsprechenden Zahl von Betriebsstunden an eine fällige Kalibrierung.

Die Ausleuchtung des LP2480zx ist mit einer Gleichförmigkeit nach VESA von gemessenen 91,2 % und einer Standardabweichung von nur 3,74 % sehr gut. Bei einer Leuchtdichte von 130 cd/m^2 beträgt der gemessene Kontrast 929:1.

Samsung XL24



Bereits Wochen vorher traf der für den professionellen Einsatz konzipierte, hardwarekalibrierbare Monitor Samsung Syncmaster XL24 im *iX*-Labor ein. Das 24 Zoll in der Diagonale messende Panel kann bei einem Seitenverhältnis von 16:10 1920 × 1200 Bildpunkte darstellen. Die Treibersoftware sorgt für die Ausgabenanpassung im Hochformat.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Zwei DVI-Eingänge (DVI-I, DVI-D), ein USB-Eingang und ein integrierter USB-Hub mit vier Ausgängen – gut zugänglich an der linken Seite des Monitors angeordnet – verbinden ihn mit der Außenwelt.

Ebenso wie der in der *iX* getestete Syncmaster XL20 [1] arbeitet der XL24 mit LED-Hintergrundbeleuchtung. Sie erreicht durch ihr relativ schmalbandiges und gut definiertes Spektrum eine hohe Farbsättigung in den Grundfarben Rot, Grün und Blau. Dadurch ist auch der Farbraum des Monitors groß genug (siehe Abbildung 2), sodass er insbesondere die im Offsetdruck darstellbaren Farben wiedergeben kann.

Zum Lieferumfang zählen die Kalibriersoftware „Natural Color Expert“ und ein passender Farbsensor. Damit lässt sich der XL24 für die Emulation unterschiedlicher Farbräume einsetzen. Standardfarbräume wie sRGB und AdobeRGB sind bereits vorbelegt. Die kann die Anwenderin laden oder die Parameter des Wunschfarbraums von Hand eingeben, etwa den für die Farbabmusterung in der Druckvorstufe empfohlenen ECIRGB-Farbraum.

Im anschließenden Kalibriervorgang stellt die Software den Monitor so ein, dass sich das gewünschte Verhalten ergibt. Die gespeicherten Farbprofile lassen sich später über eine Taste an der Frontblende aufrufen. Dadurch kann man mit dem XL24 etwa das Erscheinungsbild von Fotos und Videos jeweils in dem Zielfarbraum überprüfen, für den sie produziert werden. Je größer die Bildfläche, desto mehr rückt ein weiteres Feature der LED-Hintergrundbeleuchtung in den Vordergrund: Im Interesse einer möglichst gleichmäßigen Bildschirmausleuchtung lässt sich die Helligkeit des Bildschirms in verschiedenen Zonen messen und nachregeln, sodass sich eine gleichmäßige Ausleuchtung ergibt.

Bereits ab Werk ist die Ausleuchtung des XL24 aber schon ausgeglichen, die Gleichförmigkeit der Ausleuchtung nach VESA beträgt gemessene 90,6 %, die Standardabweichung nur 3 %. Bei einem praxisnahen Leuchtdichtewert von 140 cd/m^2 beträgt der gemessene Kontrast 920:1.

Viewsonic VLED221wm



Viewsonic bringt mit dem VLED221wm einen Monitor mit LED-Backlight in der gehobenen Büromonitorklasse. Das bedeutet, dass diese Technik nun auch bei Standardmonitoren angekommen und nicht mehr allein den teureren Bildschirmen für den Einsatz in der Druckvorstufe und anderen farbkritischen Anwendungen vorbehalten ist.

Der VLED221wm hat eine büromonitortypische Ausstattung. Sein schwarzes Kunststoffgehäuse mit glänzender Oberfläche und abgerundeten Gehäusekanten macht bereits auf den ersten Blick deutlich, dass der Monitor für die Anwendung in gehobenen Büroumgebungen gedacht ist. Der Standfuß erlaubt ein Kippen des Monitors um die horizontale Achse. In den unteren Teil des Bildschirmrahmens sind zwei Lautsprecher eingebaut.

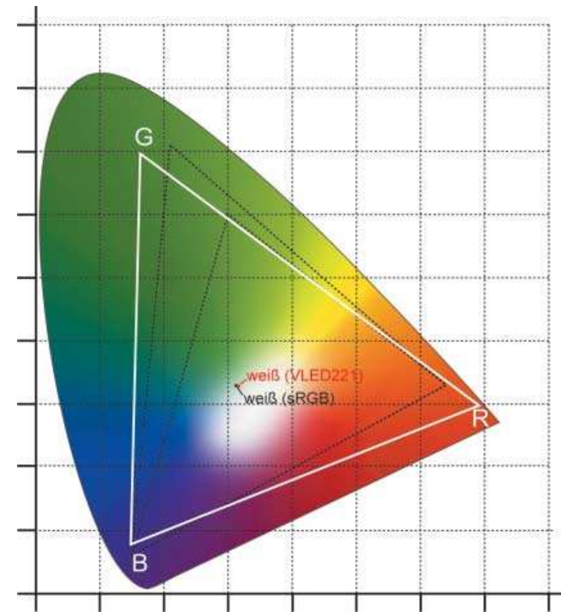
Rechts und links neben dem mittig unter dem Bildschirm angeordneten Taster zum Einschalten des Monitors befinden sich je zwei weitere zur Navigation durch die On-Screen-Menüs. Leider sind sie nur zugänglich, wenn der Monitor auch ein Signal empfängt – das kann dazu führen, dass man etwaige Konflikte mit der Grafikkarte schlechter diagnostizieren kann, weil sich dann gegebenenfalls auch die Menüsteuerung am Monitor nicht aufrufen lässt.

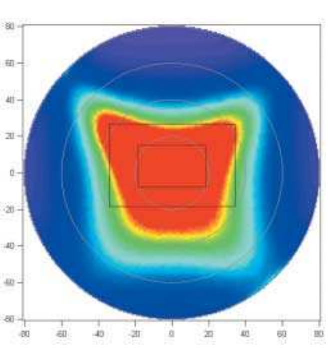
Der VLED221wm hat eine Bilddiagonale von 22" und eine native Auflösung von 1680 × 1050 – mithin also ein Seitenverhältnis von 16:10. Die HD-Auflösungsstufe 720p kann der Viewsonic-Monitor also noch eins zu eins darstellen, bei voller HD-Auflösung muss er das Bild etwas herunterskalieren.

Signale empfängt der VLED221wm analog über den üblichen 15-poligen

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.





Das native Rot ist beim Viewsonic VLED221wm deutlich stärker gesättigt als zum Beispiel für AdobeRGB erforderlich. Der Farbort des nativen Grün weicht von dem des AdobeRGB in Richtung Türkis ab (Abb. 3).

VESA-Steckverbinder (VGA-Buchse) oder digital über einen DVI-D-Eingang. Letzterer versteht auch das HDCP-Protokoll. Der Monitor unterstützt aber – vermutlich weil die native Auflösung für Full-HD nicht ausreicht – nur das Format 720p. Ist nur ein Eingang belegt, findet der Monitor automatisch das Signal, bei zwei gleichzeitig anliegenden Eingangssignalen kann man mit einem der Taster an der Vorderseite umschalten.

Dynamische Regelung des LED-Backlights

Mit dem Testpattern der Displaymate Multimedia Edition zeigte der VLED221wm keine Schwachpunkte, die Farbwiedergabe ist allerdings etwas winkelabhängig: Bei seitlichem Einblick gibt es, speziell bei dunklen Farbtönen, einen rötlichen Schimmer.

Die Farbmessungen ergeben, dass der Farbraum des VLED221wm etwas größer ist als AdobeRGB, speziell Rot ist stärker gesättigt. Die Primärfarbe Grün geht gegenüber Adobe RGB etwas stärker ins Bläuliche, das ist möglicherweise sogar Absicht, um Cyantöne, wie sie etwa im Himmelblau vorkommen, so wiedergeben zu können, wie sie auch in Offset-Druckwerken erscheinen. Die Farbtemperatur ist vom Benutzer in mehreren Stufen einstellbar.

Als Besonderheit – für einen Büromonitor – verfügt der VLED221wm über eine dynamische Regelung des LED-Backlights. Bei vorwiegend dunklen Bildpartien muss dadurch nicht allein das LCD-Panel die Abdunklung besorgen, wodurch mehr ansteuerbare Helligkeitsstufen für die Detailzeichnung in dunklen Bildpartien verbleiben. Bei schnell wechselnden Bildinhalten, etwa über DVI eingespeiste Videos, sieht man allerdings, dass die Regelung mit einer gewissen Trägheit arbeitet.

Ein solches Feature kennt man eigentlich eher von Fernsehern und Heimkinoprojektoren. Bei geeignetem Quellmaterial führt es zu deutlich verbesserten Schwarzwerten bei ansonsten kaum veränderter Bildqualität. Es gibt allerdings auch Filme, bei denen das Arbeiten der Regelung störend sichtbar wird, sodass man dann darauf lieber verzichtet. Beim VLED221wm ist es mit einem mindestens 2 s dauernden Druck auf eine der Tasten zu- und abschaltbar, sodass man es von Fall zu Fall einfach ausprobieren kann.

Die Ausleuchtung des VLED221wm ist sehr gleichmäßig, die Gleichförmigkeit der Ausleuchtung nach VESA beträgt gemessene 89,1 %, die Standardabweichung 4,2 %. Bei einer Leuchtdichte von 250 cd/m^2 beträgt der gemessene Kontrast 962:1, bei eingeschalteter dynamischer Backlight-Steuerung erhöht sich der gemessene Fullscreen-Kontrast auf 8387:1.

Fazit

Monitore mit LED-Backlight scheinen langsam erwachsen zu werden. Sie sind keine teuren Exoten mehr, die man zwar auf Messen bestaunt, aber in der Praxis nur antrifft, wenn der gebotene Mehrwert einen hohen Preis rechtfertigt. Vielmehr gibt es inzwischen ein relativ breites Angebot, das vom gehobenen Büromonitor bis zum Spezialmonitor für die Multimediabearbeitung reicht. Speziell in der letztgenannten Anwendung kann das LED-Backlight mit seinen stark gesättigten Primärfarben seine Trümpfe voll ausspielen und erlaubt zum Beispiel die Emulation verschiedener Standardfarbräume. Die Preise der getesteten Monitore entsprechen der gebotenen Leistung – ein „LED-Zuschlag“ ist nicht mehr zu erkennen. (sun)

DIETER MICHEL

arbeitet als freier DV-Journalist und ist Chefredakteur der Fachzeitschrift Prosound.

Literatur

[1] Dieter Michel; Monitore; Farbenzauber; Samsung XL20 – kalibrierbarer TFT-Monitor mit LED-Backlight; *iX* 3/2008, S. 92

Daten und Preise

HP Dreamcolor LP2480zx

technische Daten: 24"-Monitor, Widescreen 16:10; 1920 × 1200 Bildpunkte; 2 × DVI-I, HDMI (mit HDCP), Displayport, YUV (YPbPr), S-Video, Composite-Video; 4 × USB 2.0 Downstream, 1 × USB 2.0 Upstream; Pivotfunktion

Lieferumfang: Schnellstartanleitung, Netzkabel, CD (Treiber, Handbuch, Fernbediensoftware), DVI-Kabel, optional: HP Dreamcolor Advanced Profiling Solution (199 Euro netto)

Preis: 2299 Euro UVP

Samsung XL24

technische Daten: 24"-Monitor, Widescreen 16:10; 1920 × 1200 Bildpunkte; DVI-D, DVI-I, 4 × USB 2.0 Downstream, 1 × USB 2.0 Upstream; Pivotfunktion

Lieferumfang: Schnellstartanleitung, Netzkabel, CD (Treiber, Handbuch), DVI-Kabel, abnehmbarer Sichtschutz aus Aluminium, Kalibriersystem (Sensor X-Rite Eye-One Display 2, Kalibriersoftware Samsung Natural Color Expert)

Preis: 1680 Euro UVP

Viewsonic VLED221wm

technische Daten: 22"-Monitor, Widescreen 16:10; 1680 × 1050 Bildpunkte; 15-Pin Mini D-sub, DVI-D (mit HDCP), Audio (3,5 mm Klinke, stereo)

Lieferumfang: Netzkabel, 15-pin VGA Videokabel, DVI-D-Kabel, Audio-Kabel, Schnellstart-Anleitung, Viewsonic Wizard CD-ROM (Handbuch/Treiber, mehrsprachig)

Preis: 394 Euro UVP



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



VMware Fusion 2.0 für Intel-Macs

Regelmäßige Schnappschüsse

Jörg Riether

Nach einem Jahr Entwicklungszeit stellt VMware die zweite Version seines Desktop-Virtualisierers Fusion für Mac OS X vor. Hinter seiner generalüberholten Oberfläche stecken etliche neue Funktionen.

Anfang August 2007 erblickte Fusion 1.0 das Licht der Welt und beendete damit die lange Wartezeit all derer, die VMware auf dem Mac betreiben wollten. Ein gutes Jahr später und wie üblich nach einer Beta- und Release-Candidate-Phase brachte VMware die finale Version von Fusion 2.0 heraus. Fast erkennt man den Vorgänger nicht mehr wieder, denn der Hersteller hat nahezu alles visuell generalüberholt. Es fängt bei den neuen Interfaces für die Konfiguration und die Bibliothek von Gastsystemen an, die mit Fusion 1.0 kaum noch etwas gemeinsam haben (siehe Abbildung auf der folgenden Seite unten).

Die Sicherheit dürfte bei der Entwicklung eine primäre Rolle gespielt haben, denn eine der Neuerungen ist das neue Multisnapshot-Feature gepaart mit Autoprotect. Dahinter verbirgt sich der von den Anwendern lange geforderte Snapshot-Manager, der jetzt mehrere Snapshots von einer virtuellen Maschine erstellen und verwalten kann. Außerdem integrierte VMware einen neuen Automatismus namens Autoprotect, mit dem der Benutzer Snapshots in einem selbst definierten Intervall automatisch erstellen lässt. Ein Aufräumprozess rundet dieses Feature ab: Er entfernt bei Erreichen eines ebenso definierbaren Schwellenwerts veraltete Snapshots und gibt somit den verwendeten Speicherplatz wieder frei. VMware integriert auf diese Weise quasi eine eigene Time Machine in Fusion 2.0. Hinzu kommt ein komplettes Abo für McAfees Virus Scan Plus für ein Jahr – damit liefert VMware eine leistungsfähige Anti-Virus- und Anti-Spyware-Lösung für Windows gleich mit. Der Clou dabei: Die Software ist fest in Fusion 2.0 integriert, und man kann sie direkt aus dem Befehlsmenü heraus auf Knopfdruck installieren.

Auch den Arbeitskomfort hat VMware verbessert. Ein neues Feature namens Driverless Printing stellt sicher, dass man zukünftig keine Druckertreiber mehr in den Gästen installieren muss, wenn der Host selbst einen installierten Drucker besitzt. Fusion 2.0 leitet die Instruktionen automatisch auf den Host-Drucker um. Endlich unterstützt es echten Multi-Monitor-Betrieb vollständig. Dies hat man sogar so weit getrieben, dass auch „Unity“ davon profitiert, eine bereits mit Fusion 1.0 eingeführte Darstellung, bei der aktive Gast-Programmfenster direkt unter Mac OS X erscheinen, als seien sie echte Mac-Applikationen. Im Test ließ sich ein Unity-Fenster ohne besondere Konfiguration über mehrere Monitore hinweg verschieben. Etwaige Einrichtungen oder spezielle Konfigurationen sind für den Mehrschirmbetrieb nicht notwendig. Die angeschlossenen Monitore am Host erkannte Fusion völlig unspektakulär und zeigte sie in der virtuellen Maschine als solche an.

Applikationen kreuzweise öffnen

„Application Sharing“ vermag Dokumente direkt aus dem Mac-Finder in einer virtuellen Windows-Maschine zu öffnen und umgekehrt. Das funktio-

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

niert jedoch nur mit Windows als Gastsystem. Außerdem lassen sich bestimmte Schlüsselverzeichnisse unter Windows XP und Vista (Desktop, Dokumente, Bilder, Musik) direkt auf ihre Mac-Pendants mappen. Schließlich kann man URLs umleiten: zum Beispiel in einer virtuellen Maschine einen Link anklicken, den Safari auf dem Host öffnet. Umgekehrt funktioniert dies ebenso. Fusion kommt hierbei mit den URL-Typen http, https, telnet, ssh, mailto, ftp, sftp, feed und news zurecht.

Andere Maschinen intakt importieren

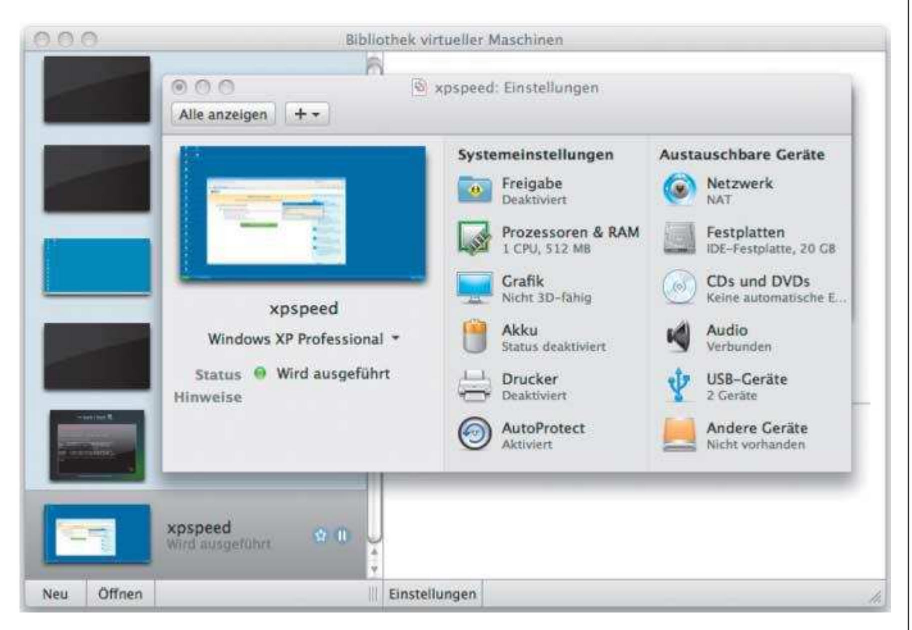
Auch im Bereich Grafikbeschleunigung hat VMware spürbar nachgelegt. Fusion ist mit DirectX 9.0c und Shader-Model2-Software kompatibel. Das Importieren einer fremden virtuellen Maschine gelingt direkt aus der Hauptapplikation heraus; im Menüpunkt „Ablage“ findet sich die neue Option „Importieren“. Auf diese Weise lassen sich virtuelle Maschinen der Konkurrenten Parallels Desktop und Virtual PC (Microsoft) importieren. Der Prozess ist nicht-destruktiv, das heißt es entsteht eine komplett neue Fusion VM, die alten Dateien bleiben unangetastet und sind weiterhin mit dem Konkurrenzprodukt nutzbar. Unity funktioniert jetzt auch mit Linux-Gästen. Das Feature hatte zwar zum Release-Zeitpunkt noch den Status „experimentell“, ließ sich aber im Test mit einem Ubuntu-„Hardy Heron“ auf Anhieb nutzen.

Eine echte Überraschung ist die Unterstützung von bis zu vier virtuellen CPUs pro Gastsystem. Damit eröffnen sich für den Otto-Normalbenutzer zwar wenige spannende Dinge, für den IT-Profi jedoch, der unter Umständen spezielle leistungsstarke virtuelle Maschinen simulieren möchte, ergeben sich dadurch interessante Möglichkeiten. Beim Thema CPU fällt übrigens eines sofort ins Auge: Wenn man hin- und wieder einen Blick auf die Mac-Aktivitätsanzeige wagt, bleibt es dort erstaunlich ruhig. Ein virtualisiertes Windows XP SP3 mit laufenden Office-Anwendungen verpulverte während des Tests auf einem Macbook Pro mit Santa-Rosa-Chipsatz im Schnitt nur 5 % CPU-Leistung.

Mehr Automatismen per Kommandozeile

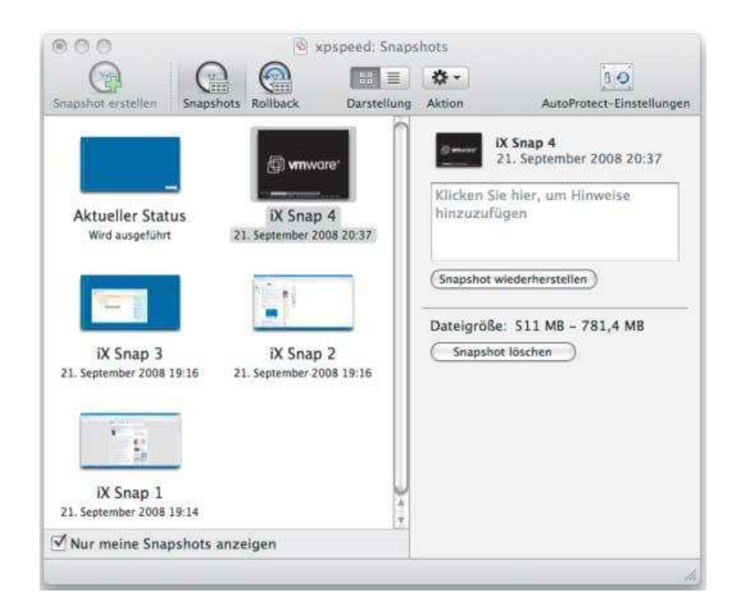
Auf der Kommandozeile hat sich endlich etwas getan. VMware bringt mit Fusion 2.0 die von der Workstation bekannten VMrun-Skripte auf den Mac. Damit lassen sich virtuelle Maschinen zum Beispiel starten, herunterfahren, anhalten oder Snapshots erstellen – insbesondere für selbst kreierte Automatismen eine segensreiche Einrichtung. VMrun ist jedoch nach der Fusion-Installation merkwürdigerweise nicht sofort aus einem beliebigen Terminal Fenster heraus benutzbar. Zunächst muss das Fusion-


Anzeige



In Fusion 2.0 sind das Konfigurations-Interface und die Bibliothek komplett überarbeitet.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Lang erwartet, jetzt integriert: der neue Snapshot Manager in Aktion.

Verzeichnis von Hand zum Systempfad hinzugefügt werden. Dies erledigt folgende Kommandozeile:

```
export \
PATH=\
"$PATH:/Library/Application Support/↵
                        VMware Fusion".
```

Danach kann man in diesem Terminalfenster *vmrun* starten, das ohne Argumente eine Liste aller Optionen zurückliefert. Für dauerhafte Änderungen sollte der Fusion-Pfad bei Leopard in */etc/paths* oder */etc/paths.d* stehen (siehe *man path_helper*). Bei älteren OS-X-Versionen übernimmt */etc/profile* eine ähnliche Funktion.

Zahlreiche Fusion-Benutzer kritisierten seit Langem das Fehlen des *vmdkmounter* auf dem Mac, mit dem man virtuelle Festplatten offline in das Host-System einhängt. Fusion 2.0 bringt es endlich mit. Auch andere alte Bekannte vom PC wie den *vdiskmanager* findet man. Der interessierte Kommandozeilen-Nutzer sollte unbedingt einen tieferen Blick in das Verzeichnis */Library/Application Support/VMware Fusion* riskieren.

Virtueller Mac nur als Server

Eine weitere Neuerung von Fusion 2.0 stellt die Möglichkeit der Virtualisierung von Leopard Server dar. Dieses Feature gilt zurzeit noch als experimentell, dennoch gelang die Installation im Test schnell und ohne Schwierigkeiten. Es waren keinerlei Unterschiede zum physisch installierten Leopard Server feststellbar. Selbst in der Maximalausstattung mit vier virtuellen CPUs und 8 GByte Hauptspeicher hatte der virtuelle Server nichts auszusetzen. Bislang gestattet Apple nur die Virtualisierung des Leopard-Server, nicht der Desktop-Variante.

Trotz zahlreicher Annäherungen auf beiden Seiten – Workstation (VMwares Desktop-Virtualisierer für PC und Linux) und Fusion bleiben weiterhin zwei unterschiedliche Produkte. Bestimmte Fähigkeiten der aktuellen Workstation sind noch nicht in Fusion integriert, beispielsweise Enhanced Execution Record/Replay, Virtual Machine Teams und die Möglichkeit der Videoaufzeichnung. Auf der anderen Seite beherrscht Fusion einiges, was der Workstation bislang fehlt: Virtualisierung von Leopard Server, Autoprotect sowie die Integration einer Anti-Viren- und Anti-Spyware-Lösung. Ob Fusion und Workstation irgendwann in der Zukunft zu einem Produkt verschmelzen, bleibt deshalb noch reine Spekulation.

Fazit

Fusion 2.0 bringt viele Detailverbesserungen sowie einige echte Neuerungen mit. Insbesondere das Autoprotect-Feature ist eine sinnvolle Idee, die VMware obendrein benutzerfreundlich umgesetzt hat. Dass der Hersteller von Käufern der Vorgängerversion nach über einem Jahr Entwicklungszeit und deutlichem Zuwachs an Fähigkeiten keinen Cent für die neue Version verlangt, ist ein feiner Zug – daran könnten sich andere Softwarehersteller gern ein Beispiel nehmen. Durch die Integration zahlreicher von der Workstation bekannter Kommandozeilenwerkzeuge dürfte Fusion auch für Tüftler mehr Reize entwickeln. Insgesamt hinterlässt die Version 2.0 einen stabilen und ausgewachsenen Eindruck. (ck)

iX-Wertung

⊕ multiple Snapshots und Autoprotect
⊕ Anti-Virus-Integration
⊕ Virtualisierung von Leopard Server
⊕ Kommandozeilen-Tools an Bord

Daten und Preise

Webseite: www.vmware.com/de/products/fusion

Preis: 79,99 €, Upgrade von Version 1.x kostenfrei

Systemvoraussetzungen: Intel-Mac mit mindestens 1,5 GHz, 1 GByte RAM (2 GByte empfohlen), Mac OS X 10.4.11 oder höher, 400 MByte Plattenplatz für Fusion, mindestens 5 GByte für jede virtuelle Maschine

JÖRG RIETHER

ist spezialisiert auf die Bereiche IT-Sicherheit, Hochverfügbarkeit und Virtualisierung. Er arbeitet als Abteilungsleiter der EDV bei der Zentrum für Soziale Psychiatrie Haina gGmbH.

Literatur

[1] Jörg Riether; Virtualisierung; Apfelpflücken; VMwares Fusion 1.0 – Final Release der Virtualisierungssoftware für Intel-Macs; *iX* 10/07, S. 72

[2] Jörg Riether; Virtualisierung; Apfelwurf; Fremdgehen auf Mac OS X mit VMwares Fusion oder Parallels’ Desktop; *iX* 5/07, S. 82

[3] Jörg Riether; Virtualisierung; Auf dem Sprung; Parallels’ Server auf dem Mac; *iX* 09/08, S. 70

[4] Jörg Riether; Virtualisierung; Gäste für Äpfel; Parallels’ Desktop 3.0 für Mac OS X; *iX* 08/07, S. 84

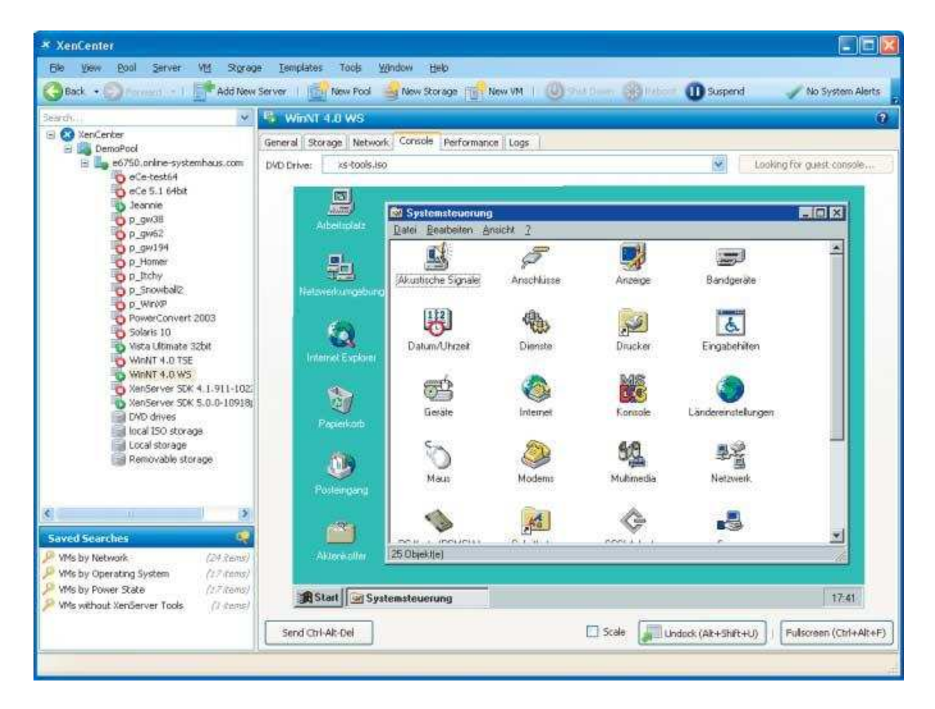




© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Citrix Xenserver 5

Virtuelle Fenster

Fred Hantelmann

Knapp ein Jahr nach der Übernahme von Xensource verkündete Citrix die Fertigstellung seines Xenserver 5.0.0. Etwa 130 Neuerungen rechtfertigen laut Hersteller den Versionssprung.

Citrix Xenserver 5 basiert auf Version 3.2.1 des Open-Source-Hypervisors Xen, bereichert um einige Rückwärtsportierungen aus dem aktuellen Xen 3.3. Die Verwaltungsinstanz (Dom0) entstammt der CentOS-Release 5.2. Als Steuerkonsole dient das proprietäre Werkzeug *xe*, das mit dem Hypervisor via XenAPI kommuniziert. Für die hostübergreifende Steuerung ganzer Farmen oder Cluster mit Xenserver liefert Citrix den Windows-Client Xencenter mit. Erweiterte Unterstützung aktueller Storage-Produkte und erstmalig verfügbare HA-Funktionen sollen die bisher vom Marktführer VMware beanspruchten Alleinstellungsmerkmale egalisieren.

Sein herausragendes Merkmal besteht laut Citrix darin, dass das Produkt als erste Server-Virtualisierungslösung am Markt einen für Microsoft zertifizierten Hypervisor enthält: Konformität zu deren Server Virtualization Validation Program (SVVP) verleiht dem Kunden das Recht, Microsofts vollständigen Support im Einsatz von Windows Server 2008, 2003 SP2 und 2000 SP4 auf der virtualisierten Hardware in Anspruch zu nehmen.

Die Steuerungsinstanz Dom0 hat Citrix um das Kommandozeilen-Verwaltungstool *xsconsole* ergänzt (siehe Abbildung). Damit kann der Administrator hostspezifische Einstellungen auch ohne Xencenter vornehmen. Performancedaten, also Auslastungsmetriken zu CPU, Speicher, Netz- und Platten-I/O, verwaltet Xenserver nun lokal in sogenannten Round-Robin-Datensätzen (RRDS), sodass die Ressourcennutzung einzelner VMs und Hosts über einen längeren Zeitraum sichtbar ist. Statt der bisher auf die letzten 15 Minuten beschränkten Übersicht kann der Administrator Daten aus einem variablen Zeitintervall abfragen, das zwischen 10 Minuten und einem Jahr lang sein darf.

Viele Wege führen zum Speicher

Wer FC- oder iSCSI-basierte Speichernetze einsetzt, profitiert in Xenserver 5 vom standardmäßig unterstütztem Multipathing. Laut Handbuch unterstützt es ein Load Balancing zwischen den vorhandenen HBAs eines Host. Eine Nachfrage beim Hersteller ergab, dass die neuen Treiber für HBAs von Emulex und Qlogic auch Failover beherrschen.

Neben Netapp-Filern, die unter Ontap 7G laufen, kommt Version 5 auch mit Dells Equalogic-Filern zurecht. Sie stellen jeder VM den Speicher als eigene LUN bereit. Plattenpartitionen des Gasts bildet der Treiber dabei auf „Sparse Files“ ab, deren Größe mit dem tatsächlichen Platzbedarf wächst. Außerdem beherrscht der Filer von Haus aus Snapshots, mit deren Hilfe sich virtuelle Maschinen schnell klonen lassen. Dazu muss der Treiber auf proprietäre Schnittstellen des Speichersystems zurückgreifen.

Physische Netzschnittstellen lassen sich bündeln (NIC-Bonding), sodass in diesem Bereich redundante Hardware für den ausfallsicheren (active/passive) Betrieb konfigurierbar ist. Ergänzend kann man ein Source Level Balancing (SLB) NIC-Bonding einstellen, das in der active/active-Betriebsart den Netzverkehr der VMs auf die Schnittstellen verteilt. Konzeptionell unterscheidet Xenserver nun zwischen internen, externen und gebündelten („bonded“) Netzen. Eine Trennung der virtuellen Hardware in NICs und Switches nimmt die Software nicht vor.

Hochverfügbarkeit (HA) unterstützt Xenserver insoweit, als Gäste in einem Host-Pool „geschützten“ Betrieb erlauben. Voraussetzung dafür ist ein FC- oder iSCSI-Speichernetz, das die virtuellen Platten eines zu schützenden Gasts verwahrt. Ein Heartbeat prüft zyklisch, ob ein geschützer Gast auf seinem angestammten Host arbeitet. Fällt der aus, startet die HA-Schicht den Gast auf einem anderen neu.

Das Aufrüsten vorhandener Xenserver-4.1-Instanzen gelang per Update-Funktion sowohl auf Stand-alone-Servern als auch auf im Pool zusammengefassten Hosts ohne Nebenwirkungen. Auf Letzteren lässt sich das Update zunächst

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

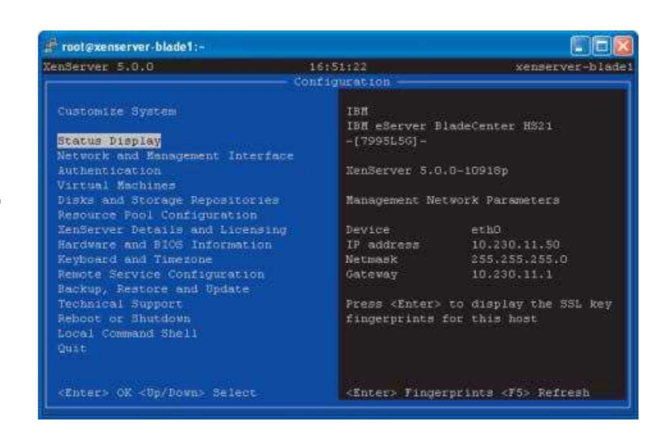
iX-Wertung

⊕ SVVP-konform

⊕ unterstützt redundante I/O-Komponenten

⊕ Enterprise-Version unterstützt Hochverfügbarkeit

⊖ keine virtuelle SCSI-Hardware für VMs



Steuerpult: Mit *xsconsole* kann der Administrator hostspezifische Einstellungen vornehmen.

ohne Unterbrechung der Gäste durchführen. Anschließend muss der Administrator aber noch die Xentools der einzelnen Gäste auf den neuen Stand bringen, was einen Neustart der Windows-Gäste erfordert.

Probehalber kamen im Test Solaris 10 und Windows NT 4 zum Zuge. Während Solaris erwartungsgemäß auf Anhieb funktionierte – auf Microsofts Hyper V gab es kürzlich im Test Unverträglichkeiten mit deren Netzwerktreiber [1] –, war die erfolgreiche Installation von NT 4 Workstation und Terminal Server Edition (ohne Service Pack) eine Überraschung – auch für Citrix. Ein Treiber für die emulierte Realtek-Netzwerkkarte 8139 verhalf den Gästen sogar zu Netbios- und TCP/IP-Kommunikation – leider nur auf einem Einprozessor-Board mit Core-2-Prozessor, jedoch nicht auf einer IBM HS21 Blade mit zwei Xeon-CPUs.

Fazit

Xenserver 5 enthält fast alle Funktionen, die beim Test seines Vorgängers [2] noch auf der Wunschliste standen: Treiber für FC- und iSCSI-HBAs beherrschen Multipathing, Performancedaten verwahrt das System über einen Zeitraum von bis zu zwei Jahren, und HA-Support zählt in der Enterprise-Version zum Lieferumfang. Auch Netzwerkkarten kann der Anwender im Verbund betreiben; wahlweise für balancierten Netzverkehr oder mit dem Ziel der erhöhten Ausfallsicherheit der beteiligten Hardwarekomponenten. Interne Erweiterungen unterstützen außerdem die Replikation von Storage-Repositories, sodass Aufbau und Betrieb von Disaster-Recovery-Sites mit geringem Aufwand gelingen.

Professionellen Anwendern dürfte die besiegelte SVVP-Konformität endgültig die Scheu vor dem Einsatz des Produkts nehmen, da virtuelle Xenserver-Hardware nun eine zertifizierte Plattform für die drei jüngsten Server-Betriebssysteme aus Redmond bildet. Bereits verfügbare Zusatzprodukte von Citrix, namentlich Xendesktop für den zentralen Betrieb virtueller Desktops und der Provisioning Server als Managementsystem für schnellen Server-Rollout, heben das Einsatzpotenzial für Xenserver 5 auf ein zeitgemäßes Niveau.

Xenserver 5 ist wie seine Vorgänger als kostenlose Express-Version erhältlich. Die Standard-Edition ist für 990 US-Dollar zu haben, Enterprise- und Platinum-Version kosten 3300 beziehungsweise 5500 Dollar. Wer die Enterprise-Edition kostenlos testen möchte, findet auf Citrix' Website (siehe *iX*-Link) eine 30 Tage lauffähige Testversion. (mr)

DR. FRED HANTELMANN

ist als IT-Architekt bei der Online Systemhaus ES+C GmbH tätig.

Literatur

[1] Fred Hantelmann; Virtualisierung; Halbrund; Microsofts Virtualisierer Hyper V; *iX* 8/2008, S. 66

[2] Fred Hantelmann; Xen; Deckmäntel; Kommerzielle Virtualisierer: XenServer und Virtual Iron; *iX* 6/2008, S. 67







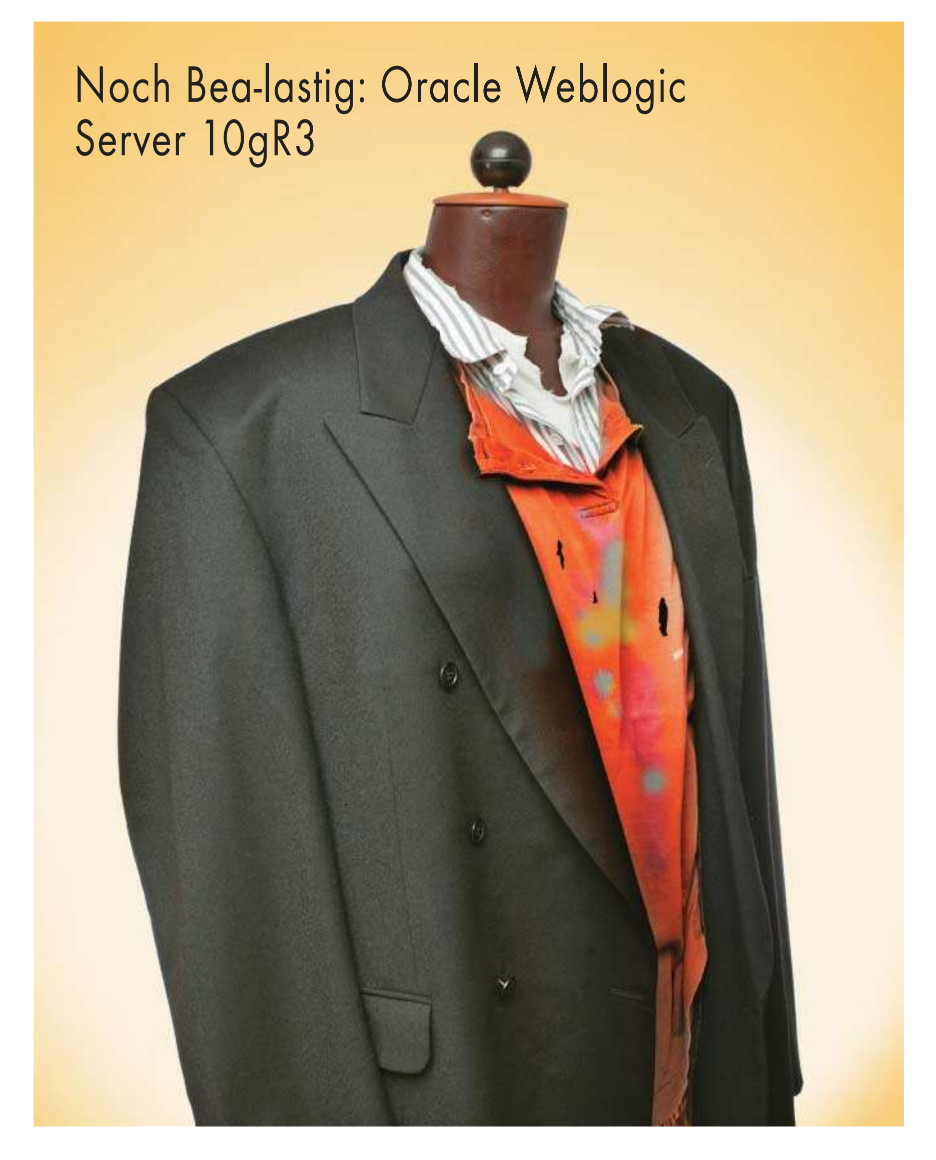
© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Noch Bea-lastig: Oracle Weblogic Server 10gR3

Neuer Anzug

Markus Eisele

Knapp ein halbes Jahr nach der Übernahme von Bea präsentiert Oracle den ersten Weblogic Server mit angepasstem Logo. Er soll künftig als neues Flaggschiff die Fusion-Middleware-Produktflotte anführen und den bisherigen hauseigenen Applikationsserver versenken.

Schon Ende letzten Jahres konnten sich Interessierte mit der Technology Preview des Weblogic Server beschäftigen. Erst Mitte 2008 tat sich Neues: Oracle verschob die Entwicklerwebseiten der aufgekauften Bea (dev2dev, arch2arch et cetera) in das eigene Technology Network (OTN) und stellte unmissverständlich klar, dass die Produkte der Weblogic-Server-Reihe in der Fusion Middleware aufgehen sollen und somit die künftige Basis aller hauseigenen JEE-Produkte bilden.

Die nun mit dem Namen Weblogic Application Server 10gR3 versehene Minor-Release verspricht keine bahnbrechenden Neuerungen (wofür das „g“ in diesem Zusammenhang steht, bleibt weitgehend unklar). Vielmehr wollte man den seit der 9er-Version ziemlich aufgeblasenen Server (bis zu 950 MByte als Gesamtpaket) wieder auf das Volumen seiner Vorgänger schrumpfen. Mit 750 MByte gibt sich die aktuelle Distribution auch deutlich schlanker. Wer das immer noch als zu mächtig empfindet, sollte direkt mit dem Net-Installer arbeiten, der die gewünschten Teile selektiv lädt und einrichtet.

Neben dem obligatorischen Kern kann der Entwickler neun weitere Komponenten installieren (er muss aber nicht). Zur Auswahl stehen die browserbasierte Administrationskonsole, verschiedene Client-Pakete, Plugins, Beispielanwendungen, JDBC-Treiber sowie die Entwicklungsumgebung Workshop. Ob er eine vorhandene Java Virtual Maschine (JVM) verwenden will, steht ebenfalls im Ermessen des Anwenders. Ansonsten liefert Weblogic wahlweise die hauseigene JVM JRockit oder die Standard-JVM von Sun mit. Durch diese Maßnahmen gewinnt der Server vor allem an Geschwindigkeit. Das Starten und Stoppen der Instanzen geht schneller von der Hand als beim Vorgänger und der Speicherverbrauch ist deutlich gesunken.

Von Haus aus benutzt Weblogic das Java Development Kit 1.6. Er gibt sich zwar auch mit 1.5 zufrieden, das aktuelle JDK bringt jedoch einen Zuwachs an Performance von 10 bis 15 Prozent. Nebenbei bietet es weitere Vorteile, etwa ein besseres Thread-Handling. Das Produkt enthält nun die Java Scripting API (JSR-223), die dem Webcontainer die Kooperation mit PHP, Groovy und Ruby ermöglicht.

An den Programmierer gedacht

Vor allem für die Anwendungsentwickler bietet der neue Application Server mehr als die Version 9. Mit Letzterer musste man nach kleinen Modifikationen stets ein komplettes Deployment inklusive Server-Neustart durchführen. Die Funktion *FastSwap* erlaubt nun, einzelne Klassen zur Laufzeit auszutauschen, die Änderungen sind nach dem Neuladen der entsprechenden Seite sofort sichtbar. Der bisher eingesetzte *ChangeAwareClassLoader* baute den

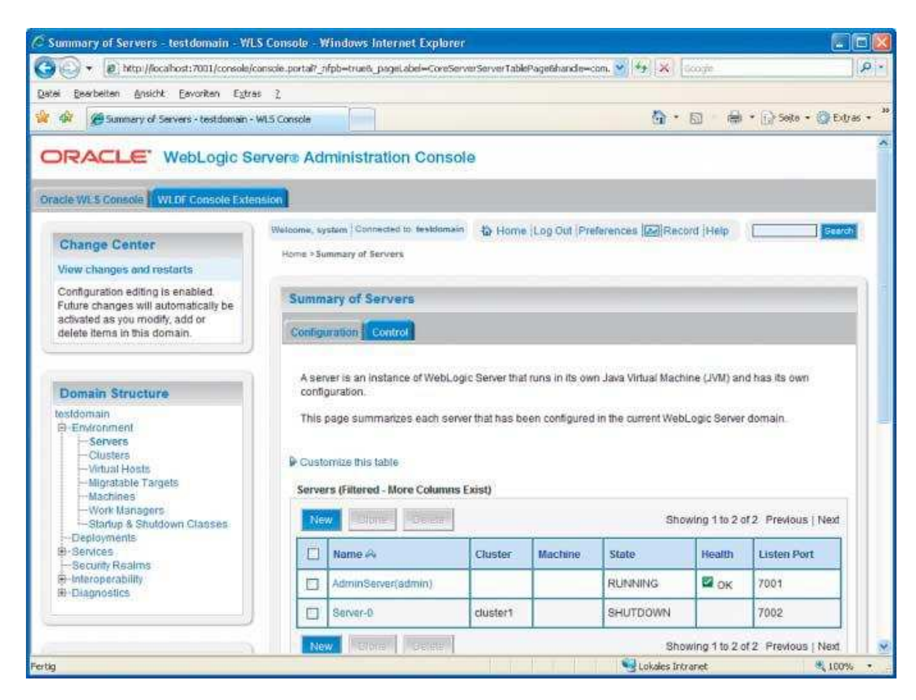
© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Classloader jedes Mal neu auf und verlor dabei seinen Serverkontext. *FastSwap* funktioniert nur im Development-Modus, im Produktionsmodus ist es nicht erreichbar. Der Austausch der Klassen lässt sich nur bei entpackten Programmen (exploded Mode) anwenden. Eingeschaltet wird die Funktion im zugehörigen Deployment Deskriptor (*weblogic-application.xml*), hier setzt man *<fast-swap>true</fast-swap>*.

Bea bot zwei Weblogic-Distributionen an: WLS enthielt den kompletten JEE-Server mit allen Containern und Funktionen, die abgespeckte WLX begnügte sich mit dem Webcontainer und verzichtete auf EJB, JMS et cetera. Technisch waren die beiden Varianten identisch, es gab lediglich unterschiedliche Lizenzschlüssel. 10gR3 lässt sich hingegen in zwei verschiedenen Konfigurationen starten, über die Option *-DserverType=* kann man entweder *wlx* oder *wls* wählen. Jeder Servertyp startet nur die Dienste, die er tatsächlich benötigt.

Neben der Administrationskonsole liefen bisher im Server der UDDI Explorer, Webservice- und Async Dispatcher Servlets sowie der WLS-Testclient. 10gR3 richtet diese Anwendungen nur noch bei Bedarf (im Entwicklungsmodus) ein. Beim erstmaligen Zugriff auf beispielsweise das Verwaltungswerkzeug erscheint eine Meldung, dass der Server es gerade „deployed“. Der Produktionsmodus installiert und startet die genannten Programme bereits beim Anlaufen des Servers.

Nachdem Bea die Verwaltungskonsole in der Version 10.0 auf das Portal-Framework umgestellt hatte, erschlug sie den Administrator förmlich mit ihrer unvorstellbaren Menge an Funktionen. Oracles Ausführung rückt hier einiges zurecht. Das Werkzeug baut sich schnell auf und die Bedienung ist wieder durchschaubar. Es gibt kleine Hilfsprogramme wie „Fenster minimieren/maximieren“ und der Einsatz des nervigen Change Centers ist nun optional. Wer darüber Änderungen vornehmen wollte, musste bislang die Systemkonfiguration für andere Nutzer explizit sperren. Diese Funktion hat Oracle jetzt standardmäßig ausgeschaltet, sie lässt sich bei Bedarf jedoch aktivieren. Veränderte Systemeinstellungen sind somit sofort aktiv. Bei den neu eingeführten Erweiterungen (console extensions, über *Preferences* ein- und auszuschalten) sticht vor allem die Konfiguration des Java-Famework Spring hervor.



Hinter der Oracle-Fassade verbirgt sich noch das altbekannte Original des Weblogic Server.

Schneller mit schnittigem Outfit

Gefühlt ist die nun im Oracle-Design gehaltene Konsole, auf der sich kein Hinweis mehr auf den Originalhersteller finden lässt, bis zum Faktor drei schneller geworden (siehe Abbildung oben). Hauptsächlich dafür verantwortlich zeichnen die verbesserten Portalfunktionen (etwa Multi-threaded Backing Files).

Bei den Erweiterungen der Java EE stehen die neuen Versionen rund um Java Webservices (JAX-WS) 2.1 im Vordergrund. Vor allem die Unterstützung für SAML2 (Security Assertion Markup Language) fällt ins Gewicht. Der Server kann mit sämtlichen Webservices-Standards von OASIS wie WS-Security, WS-Policy, WS-Reliable Messaging und WS-Addressing umgehen. Für deren Verwaltung spendierte man der Administrationskonsole eine neue Seite. Gemeinsam mit Microsoft erleichterte der neue Eigner die Zusammenarbeit zwischen Weblogic-Webservices und denen von der Microsoft Windows Communication Foundation (WCF) 3.0 erstellten.

Die JEE5-Spezifikation führte Dependency Injection (DI) für Web- und EJB-Container ein. Weiterhin findet man jetzt Interceptors (ein Konzept der aspektorientierten Programmierung, AOP) im EJB-Container. Der Entwickler denkt dabei natürlich an Spring. Um DI und Interceptors zu vereinen, starteten Bea und Springsource bereits Anfang 2007 das Projekt Pitchfork, das in Oracles Weblogic Server die Koordination übernehmen kann, wenn es der Admin explizit einstellt. In der Standardinstallation benutzt Weblogic die von der JEE-Spezifikation vorgegebenen DI- und Interceptor-Optionen.

Am Web 2.0 kommt auch Weblogic nicht vorbei. Er bietet einen HTTP-

iX-TRACT

- Weblogic Server 10gR3 ist der erste Application Server, der nach Beas Übernahme durch Oracle unter der Regie des neuen Eigners erscheint.
- Einige der Macken des 10er-Ausführung des Bea-Servers hat Oracle beseitigt, beispielsweise ist die neue Release kleiner und schneller.
- Von einer Zusammenführung mit Oracle-Technik kann noch keine Rede sein, unter der neuen Oberfläche steckt noch weitgehend das bekannte Bea-Produkt.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Publish-Subscribe-Server zum Verarbeiten von Ajax-Anfragen, und Oracle stärkte die Webentwicklung: Einzelne Sessions lassen sich debuggen und ein entsprechendes Flag im Deployment Descriptor stellt das Logging von erweiterten Session-Informationen sicher. Der Webcontainer wurde ebenfalls modernisiert, im Cluster lassen sich Sessions nun asynchron zwischen Primary und Secondary Server replizieren.

Auch bei der Sicherheit hat sich etwas getan. Der bislang obligatorische, eingebaute LDAP-Server lässt sich nun vollständig durch ein Datenbanksystem ersetzen, was das Verankern des Servers in Identity-Management-Infrastrukturen deutlich vereinfacht. Als bemerkenswerte Neuerung fällt die C#JMS-Client-Bibliothek für .Net auf. Die API ermöglicht es .Net-Anwendungen, ohne speziellen Java-Client auf direktem Wege mit Weblogics JMS-Subsystem zu kommunizieren.

Nach der Würdigung des Servers fehlt noch der kritische Blick auf die Entwicklungsumgebung Workshop, die man bisher separat erwerben musste. Nun darf man sie kostenlos mit anderen Plattformen einsetzen. Neben Weblogic kooperiert der Workshop mit IBMs Websphere, Apaches Tomcat, JBoss, Jetty und Resin. Er basiert jetzt auf Eclipse 3.3 sowie der Web Tools Platform 2.0 (WTP), läuft auch unter Windows Vista und kennt alle aktuellen JEE5-Standards, darunter Servlet 2.5, JSP 2.1, JSF 1.2, JSTL 1.2. Zudem beherrscht er Design, Build und Deployment mit separaten Views für alle Weblogic-Belange und enthält Werkzeuge für die genannten Webservices-Standards. Bei Java Server Faces hat der Entwickler die Wahl zwischen Suns Referenzimplementierung oder Apaches Myfaces. Leider kann der neue Workshop mit der in Version 10 erstmals gewährten Unterstützung für Adobes Flex nichts mehr anfangen.

Bleibt die Frage, wie viel Eigenanteil Oracle bereits in den Weblogic 10gR3 hineingesteckt hat. Nicht viel, denn durch die Oracle-Oberfläche schimmert der altbekannte Bea Weblogic deutlich durch, zu erkennen an den Klassen- oder Dateinamen. Selbst die Dokumentation liegt noch unter der Domain *edocs.bea.com*. Vor allem: Von einer Integration des 10gR3 in die Fusion Middleware ist noch nichts zu sehen. Laut Plan soll der neue den alten Applikationsserver erst in der Version 11 ablösen. Kein Wunder also, dass man zurzeit noch vergeblich nach Anbindungsmöglichkeiten für Forms, PLSQL, Reports, Application Developer Framework (ADF) oder Ähnlichem sucht. Für Forms wäre es vergleichsweise einfach, da die Umgebung sich kaum im JEE-Umfeld bedient. Die Hauptarbeit erledigt der Benutzer hier in der Sprache C. Lediglich ein Forms Listener Servlet vermittelt zwischen Forms Client und Server. Auch hier muss man auf 11 warten.

ADF besteht aus zwei Teilen. Zum einen unterstützt der JDeveloper das Entwickler-Framework, zum anderen gibt es die ADF Faces, als JSF-basierte Komponentenbibliothek für Webclients. Letztere übergab Oracle bereits im Januar 2006 an die Apache Foundation, sie sind nun Teil des Myfaces-Projekts. ADF Faces sollten sich somit ohne Einschränkung auf dem Weblogic Server einrichten lassen. Erst Workshop 11 wird die vollständige ADF-Integration bewerkstelligen.

iX-Wertung

⊕ unterstützt maßgebliche JEE-Standards
⊕ schneller und kleiner als Vorgänger
⊕ verbesserte Administrationskomponente
⊖ nicht mit Oracle-Technik integriert

Daten und Preise

Oracle Weblogic 10gR3 – Enterprise Edition

Systemanforderungen: 1 GHz CPU, 1 GByte RAM, 3,5 GByte Plattenplatz
Betriebssysteme: Unix, Windows, Linux
Datenbanken: DB2, Informix, Oracle, SQL Server, Sybase, Pointbase, MySQL
Preise: auf Anfrage
Anbieter: Oracle, www.oracle.com

Fazit

Oracles Weblogic Server 10gR3 entspricht noch im Wesentlichen Beas Original. Einigen der Kritikpunkte hat sich der neue Eigner jedoch gewidmet. Dank dafür gebührt wohl noch Beas Entwicklungsmannschaft. Der Server startet schnell, und über die Bedienung der Administrationskonsole kann man sich nicht mehr beklagen. Gewöhnungsbedürftig ist lediglich das neue Logo.

Onlinequellen

Oracle Weblogic Server, Download
www.oracle.com/technology/products/weblogic
Oracle Technology Network
otn.oracle.com
Dokumentation zu 10gR3
edocs.bea.com/wls/docs103/

Viele Kunden haben bereits mit Erscheinen des Weblogic 10.0 die Migration eingeleitet. Zumeist hoben sie 6.1er- oder 8.1er-Installationen auf die neue Release, vor allem deswegen, weil der Support für die älteren Versionen in vielen Fällen ausgelaufen ist. Theoretisch müsste eine auf Weblogic 10 migrierte Anwendung klaglos auch unter 10gR3 funktionieren, allerdings wird das in der Praxis wohl kaum jemand ausprobieren wollen. Die noch mit Bea getroffenen Lizenzvereinbarungen gelten weiter.

Es ist nicht damit zu rechnen, dass sich viele Kunden derzeit neue Lizenzen zulegen werden, und zwar nicht nur aufgrund der noch unfertigen Roadmap für das Produkt. Auch wenn sich die Übernahme von Bea als geschickter Schachzug erweisen sollte, bleiben Unklarheiten über die Zukunft der Software sowie der JEE-Spezifikation bestehen, die Bea jahrelang aktiv mitgestaltet hat. Spätestens wenn der Weblogic Server seine Oracle-spezifische Unterfütterung erhält und sich in die Fusion-Palette einfügt, stellt sich die Frage, ob er noch als unabhängiger JEE-Application Server seinen Dienst in anderen als Oracle-Installationen verrichten kann. (jd)

MARKUS EISELE
arbeitet im Bereich Software-Technologie im Center of Competence IT-Architecture der msg systems AG.

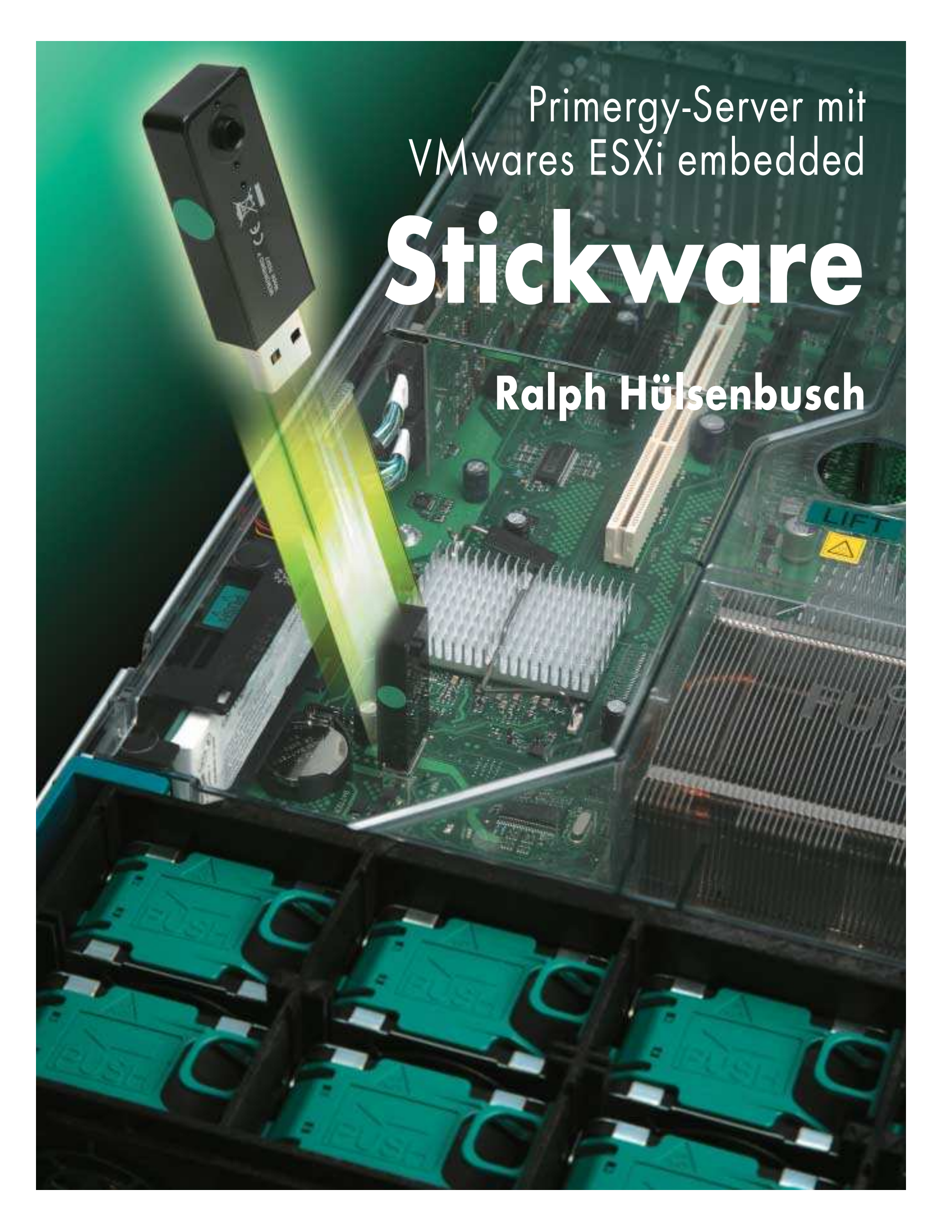
Literatur

[1] Markus Eisele; JEE-Programmierung; Neue Zeitrechnung, Weblogic Realtime 1.0: Echtzeit light; *iX* 8/2006, S. 64
[2] Markus Eisele; Application Server; Neue Basis; Weblogic Server 10 mit JEE5-Unterstützung; *iX* 7/2007, S. 76





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Primergy-Server mit VMwares ESXi embedded

Stickware

Ralph Hülsenbusch

Nach der ersten VMworld in Europa Anfang des Jahres war das Thema Virtualisierung embedded mit VMwares ESXi in aller Munde. Fujitsu Siemens Computers lieferte einen ersten Server aus deutscher Produktion mit VMwares Hypervisor on board.

Klein und fein zu sein zählt zu den Vorzügen der Virtualisierungssoftware ESXi von VMware. Im September 2007 brachte der Hersteller das Leichtgewicht auf den Markt, seit dem 28. Juli 2008 verschenkt er es nach Registrierung per Download. Der Hypervisor begnügt sich mit 32 MByte und bietet alles, was man braucht, um virtuelle Maschinen einrichten, starten und stoppen zu können. Ein geschickter Schachzug von VMware, denn zum einen hat das kräftig zur Verbreitung von deren Virtualisierungstechnik beigetragen, zum anderen jeden, der mehr will, etwa eine Migration im laufenden Betrieb, quasi zum Kauf weiterer Komponenten der VMware Infrastructure 3 (VI3) gedrängt.

Gut verpackt im kleinen Speicher

Dank des geringen Umfangs passt der ESXi auf einen handelsüblichen Flash-Speicher. Und da fast alle neueren Systeme über USB booten können, steht dem Einrichten virtueller Systeme nichts im Wege. Die Folge sind eine ganze Reihe vorgefertigter Maschinen vom BSD-, Linux-, Unix- und Windows-Server bis hin zu Datenbanken oder SAPs Business-Software. Das veranlasste VMware zur letzten VMworld [1], Kunden USB-Sticks zu schenken, auf denen ESXi bootfähig installiert ist. Und nahezu alle Systemhersteller ließen es sich nicht nehmen, „VMware ESX embedded“ zu verkünden.

Dazu zählte Fujitsu Siemens Computers, die sich beim Wort nehmen ließen und ihren Primergy Server RX300 S4 mit ESXi an Board zur Begutachtung schickten. Das solide zwei Einheiten hohe Einbau-System fürs Rack präsentiert nach dem Einschalten auf der Konsole ein Startbild, dass dem Administrator die per DHCP bezogene URL für das Web-Interface zum ESXi verrät.

Grundlegendes unter der Oberfläche

Außer zwei Funktionstasten zum Runterfahren und Konfigurieren gibt es keine weiteren Bedienelemente. Über F2 kann der Administrator grundlegende Dinge erledigen: ein Passwort setzen, im Lockdown Mode „root“ aussperren, das Netz konfigurieren und neu starten, das Keyboard auswählen, Support-Informationen abrufen wie Servicenummer, Lizenz und SSL-Thumb (SSA1), drei Arten von Log-Dateien auslesen (Infos, Cuio und Management Agents), die Management Agents neu starten und das ganze System in den Auslieferungszustand zurücksetzen. Alles in allem wenig Kompliziertes. Zum Lesen und Durchsuchen der Log-Dateien dient eine Art *vi*, bei dem aber der Zugriff auf die Shell per „:!“ gesperrt und kein Abbruch per Hot-Key möglich ist. Sämtliche Konfigurationsdaten speichert ESXi auf dem Stick.

Der weitere Weg ist geebnet, sobald man auf den Webserver zugreifen kann. Dazu bedarf es nur der richtigen Webadresse, die der Server bei Auslieferung per DHCP erhält. Unter der erscheint im Webbrowser eine Seite, auf der VMware zum Download des freien Infrastructure Client (VIC) auffordert und für das stromlinienförmige Gestalten (Streamlining) den kostenpflichtigen Virtualcenter Server sowie die Dokumentation für Infrastructure 3 anbietet. Den Client gibt es nur für Windows, für Windows und

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

VMware ESX Server 3i 3.5.0 build-00000

VMware, Inc. VMware Virtual Platform

Intel(R) Core(TM)2 Duo CPU T7500 @ 2.20GHz
1 GB Memory

Download tools to manage this host from:
http://192.168.33.129/ (DHCP)

<F2> Customize System <F12> Shut Down/Restart

Abschreiben: Nach der Konfiguration muss sich der Administrator die IP merken, denn weiter geht es per Browser von einem anderen Rechner aus.

Linux bietet VMware ein per Kommandozeile gesteuertes Werkzeug an. Das Aktivieren des zugehörigen Links führte auf eine unübersichtliche Seite, auf der man unter CLI (Command Line Interface) einen Download-Link findet. Dort liegt außer den beiden genannten Varianten noch eine weitere Zip-Datei mit einer VM, die das Kommandozeilen-Interface bereitstellt. Das ist aber nicht für den produktiven Einsatz gedacht.

Mit der grafischen Oberfläche des VIC kann der Administrator intuitiv mit dem System arbeiten, den Zugang ändern und schützen, virtuelle Maschinen (VMs) aufbauen und die Ressourcen zuweisen – ESXi halt [2]. Die grafische Benutzeroberfläche bietet einen großen Umfang an Informationen und Funktionen, der klar gegliedert und fast ausschließlich selbsterklärend ist. Für die VMs sind Konsolen erreichbar, die mit der Maus fast punktgenau synchronisieren. Das CLI hingegen kommt mit einer mageren Hilfefunktion daher und bietet rudimentäre Funktionen wie start, stop, snapshot und suspend nebst einer Statusabfrage.

Man erfährt etwas über die Ausstattung der physischen Maschine mit CPUs und Speicher, wer mehr über die Hardware wissen will, muss vor Ort nachschauen. Nach dem Öffnen der oberen Metallabdeckung im laufenden Betrieb fällt sofort ein hellblau leuchtende LED unter einer Plexiglasabdeckung des Rechners ins Auge: Sie gehört einem USB-Stick, der zwischen Chips und Datenleitungen in einem USB-Anschluss mitten auf dem Board steckt. Wer den Stick im ausgeschalteten Rechner herauszieht, hat nach dem Neustart einen betriebssystemfreien RX-Server vor sich. Auf dem 2 GByte fassenden Flash-Speicher sind vier FAT16-Partitionen untergebracht.

Device	Boot	Start	End	Blocks	Id	System
/dev/sdf1		5	750	763904	5	Extended
/dev/sdf4	*	1	4	4080	4	FAT16 <32M
/dev/sdf5		5	52	49136	6	FAT16
/dev/sdf6		53	100	49136	6	FAT16
/dev/sdf7		101	210	112624	fc	Unknown
/dev/sdf8		21	750	552944	6	FAT16

Sie erscheinen unter Linux als:

```
.hal-mtab          Hypervisor0/     Hypervisor2/
.hal-mtab-lock     Hypervisor1/     Hypervisor3/
```

Partitionen wie auf einer Platte

Jedes Hypervisor-Verzeichnis enthält unterschiedliche Inhalte. Im ersten ruhen die Grundkonfiguration, die Linux-Loader und das Boot-Image, im zweiten und dritten gepackte Dateien, im vierten das Filesysteme mit allem, was ESXi braucht. Beim Hochfahren des Rechners startet es vom Stick. Es sucht anschließend nach Updates und führt sie automatisch durch. Am 12. August 2008 gab es eine Überraschung: Die Lizenzen waren abgelaufen, da wohl jemand vergessen hatte, die Zeitbombe der Beta-Version im Update 2 aus dem Code zu entfernen. Zwar beeinträchtigte das laufende VMs in keiner Weise, aber schlafen gelegte oder runtergefahrene ließen sich nicht mehr aktivieren.

Am 13. kam ein Patch für embedded ESXi heraus, den FSC mit einer Anleitung lieferte, wie der Stick neu zu bespielen ist. Demnach geht es nicht auf dem Server, da dort kein Betriebssystem läuft, das den USB-Stick als Speicher erkennt. Irgendein Windows-Rechner mit USB-Anschluss reicht aber, um den Stick mit neuer Software zu versehen. Doch wer seine VMs nicht vorher auf einen anderen ESXi verlagert hatte – was ja ohne kostenpflichtige Erweiterungen mit VMwares Infrastructure 3 nicht geht – stand nach dem reibungslosen Booten des Servers vor dem Nichts. Sämtliche VMs waren verschwunden. Wenn man einen Server mit embedded ESXi betreiben will, muss man für ein Backup sorgen, was aber bei einem einzelnen System ohne Zusatzsoftware nicht geht.

Update auch ohne Neuinstallation

Es hätte aber einen anderen Weg gegeben. VMware liefert zum Infrastructure Client das Infrastructure Update – sofern man das passende Häkchen in der GUI beim Installieren setzt. Das Werkzeug hat VMware speziell für die Auffrischung des ESXi embedded beigelegt. Ein zweiter Versuch, im laufenden Betrieb Updates auf dem Stick durchzuführen, ging ohne besondere Vorkommnisse vonstatten. Leider übersieht man das wichtige Hilfsmittel leicht, da es zwischen ihm und dem Client keinerlei Beziehung gibt, außer dass die Icons gleich aussehen.

Im Grunde genommen kann ESXi embedded seine Stärke auf einem einzelnen Server mit lokalen Platten nicht so recht ausspielen. *iX*-Autor Sven Ahnert [3], der ESXi selbst einsetzt, sieht echte Vorteile vor allem in Umgebungen mit Speichernetzen. Dort kann man Server mit ESXi im Stick völlig ohne lokale Laufwerke betreiben. Neue Server braucht der Admin nur ans Speichernetz zu koppeln und zu konfigurieren.

Außerdem sparen Diskless-Server Strom und produzieren weniger Wärme. Ein weiteres Plus erhält die Mobilität: Der Stick lässt sich ohne Weiteres an anderen Servern betreiben. Bei einem Systemwechsel bleibt die Konfiguration erhalten. Nutzt man einen Rechner mit anderen Aufgaben, sind nur wenige Parameter umzustellen, oft reicht das Ändern der IP, sofern nicht DHCP eingestellt ist. Was für den Stick gilt, gilt selbstverständlich auch

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

für Server mit anderen Speichermedien wie Solid State Disks (SSD).

Fazit

Abgesehen von exotischen Kombination aus Rackserver und integriertem USB-Stick on board – was den Begriff von embedded arg strapaziert – bleibt ein bitterer Nachgeschmack angesichts des Update-Desasters. Schlank und frei ist der ESXi Hypervisor, aber seine Funktionen sind rudimentär. Hinzu kommt die doppelte Abhängigkeit von Windows: Einmal braucht man es, um den grafischen Client nutzen zu können, zum anderen sind fällige Patches des Sticks nur darüber möglich. Von welcher Qualität der USB-Stick selbst ist, lässt sich so nicht feststellen. Zumindest rein äußerlich unterscheidet er sich von handels- und geschenküblichen in keiner Weise – eine SSD würde vertrauenerweckender wirken.

Dem steht gegenüber, dass der Server, einmal gestartet, rund läuft und die Bedienung über den Client einfach und intuitiv ist. Eine feine Sache, wenn man mal das eine oder andere ausprobieren möchte und der Verlust einer VM keine weiteren Auswirkungen hat. Als allein stehender Server eignen sich FSCs Primergy Server RX300 S4, das Pendant mit AMD-CPU RX330 S1 oder das Standgerät TX300 S4 mit ESXi embedded für kleine Betriebe oder Außenstellen, die mehrere Server-Instanzen benötigen, anderenfalls dürfte ein „normaler“ Server geeigneter sein. Die eigentlichen Vorteile des ESXi embedded kommen jedoch erst in Verbindung mit Speichernetzen wie SAN und mehreren Servern zum Tragen. (rh)

iX-Wertung

⊕ schnelle Konfiguration

⊕ intuitive Bedienbarkeit

⊕ Einsparung von Energie und Ressourcen

⊖ Noname-USB-Stick

Daten und Preise

RX300S4 ESXi

Hardware: zwei Xeon Quad-Core L5420, 2,5 GHz; 16 GByte RAM (8 × 2 GByte); RAID 5/6, 272 GByte RAID 1, 136 GByte RAID 5; DVD-ROM; zwei Gigabit-Ethernet; Service-Prozessor; 2-GByte-USB-Stick on board

Software: ESX 3i Server 3.5 Update 2

Hersteller: Fujitsu Siemens Computers, www.fujitsu-siemens.de

Preis: ab 940 €

Literatur

[1] Jörg Riether; Virtualisierung; Über den Teich; VMworld Europe 2008; *iX* 4/2008, S. 40

[2] Jörg Riether; Neuerungen in VMwares Enterprise Suite VI 3.5; *iX* 2/2008, S. 22

[3] Sven Ahnert; Virtualisierung; Transparente Verbindlichkeiten; Stärken und Schwächen von VMwares Infrastructure 3; *iX* 9/2007, S. 70







© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Schwierigkeiten beim Erstellen barrierefreier PDFs

Hürden nehmen

Helmut Moritz

Die Technik zur Erstellung barrierefreier PDF-Dokumente ist seit drei Jahren beinahe unverändert geblieben, und es gibt nach wie vor keinen Standard dafür. Das führt zu Unmut bei Anbietern und Produzenten solcher Dokumente, da viele Fragen ungeklärt bleiben und sie Fehler in Kauf nehmen müssen. Auch Adobe hat es in der neuen Version 9 von Acrobat verpasst, die Technik zur Reife zur bringen.

Barrierefreie PDFs sollen den Zugang zum Inhalt eines Dokuments für Menschen mit Behinderungen erleichtern beziehungsweise überhaupt ermöglichen. Das erreicht man
– durch Bildschirmleseprogramme, die den Inhalt des PDF-Dokuments korrekt erkennen,
– durch die Ausgabe des Inhalts frei von optischer Gestaltung und in der korrekten Reihenfolge (dieser „Umfließen-Modus“ ist vergleichbar mit der Betrachtung einer Internetseite in einem Textbrowser) und
– dadurch, dass unter anderem Lesezeichen die Navigation per Tastatur erleichtern.

Zu diesem Zweck versehen Autoren die Elemente innerhalb eines PDF-Dokuments mit Auszeichnungen, sogenannten Tags. Für Überschriften steht beispielsweise ein <*h*>-Tag zu Verfügung, für Absätze ein <*p*>, und Listenelemente werden mit einem <*li*> ausgezeichnet. Hieraus ergibt sich der Tag-Stamm oder auch Tag-Baum. Weitere Anforderungen sind, dass das Dokument Lesezeichen enthält, wesentliche Abbildungen mit einem Alternativtext versehen sind und die Hauptsprache definiert ist. Der „Umfließen-Modus“ sieht vor, dass der Inhalt bei einer Größenskalierung weiterhin korrekt erscheint (Abbildung 1). Fehlerfrei lassen sich solche Dokumente bisher nur mit Acrobat und Indesign von Adobe erstellen.

Bisher keine Bindung an Standards

Die Erstellung von Dokumenten, die den oben genannten Kriterien entsprechen, ist schwierig und mitunter sogar unmöglich. Die Technik ist unausgereift, und es gibt keinen Standard, gegen den Autoren testen könnten. Leidtragende dieser Situation sind unter anderem öffentliche Institutionen und Dienstleister, da sie barrierefreie PDF-Dokumente anbieten oder produzieren müssen.

2002 hat die Bundesregierung erste Ansätze konkretisiert, um PDF-Dokumente zugänglicher zu machen: Die „Barrierefreie Informationstechnik-Verordnung“ (BITV) ist eine Ergänzung des Behindertengleichstellungsgesetzes und soll bewirken, dass Menschen mit Behinderungen in der Lage sind, Zugang zum Internetangebot von Behörden der Bundesverwaltung zu finden oder dass ihnen dieser Weg zumindest erleichtert wird (siehe „Onlinequellen“). Diese Verordnung gilt gleichermaßen für PDF-Dokumente.

Das Projekt „Barrierefrei Informieren und Kommunizieren“ (BIK) verfolgt das Ziel, „Webangebote besser zugänglich zu machen“. Der in diesem Rahmen entwickelte BITV-Test überprüft in regelmäßigen Abständen die Internetangebote der Bundesministerien. Die Motivation von BIK ist unter anderem, dafür zu sorgen, dass behinderte Menschen nicht mehr wie heute in vielen Fällen Texterkennungssoftware einsetzen müssen, um sich ein PDF-Dokument erschließen zu können. „Eine Navigation anhand von Strukturmarkierungen ist dann nicht mehr möglich, was dem Gleichstellungsgrundsatz widerspricht“, kritisiert Detlef Girke von BIK. Die Anforderungen des BITV-Tests an PDF-Dokumente sind umfangreich und bieten zumindest ein Regelwerk, an dem sich Anbieter und Entwickler orientieren können. Doch noch immer existiert kein verlässlicher Standard zur Optimierung eines PDFs auf Barrierefreiheit. Viele Ansätze zur Optimierung beruhen daher auf Interpretationen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Die Darstellung eines Inhaltsverzeichnisses: links im Normalmodus und rechts im Umfließen-Modus, bei dem der Inhalt einzeln pro Zeile und in der korrekten Reihenfolge ohne Schmuckelemente erscheint (Abb. 1).

Ein Inhaltsverzeichnis in der Normalansicht	Das gleiche Inhaltsverzeichnis im Umfließen-Modus (Reflow)
1. **Inhaltsverzeichnis** 2. **Überschrift erster Ebene** 1. Überschrift zweiter Ebene 2. Überschrift zweiter Ebene ▪ Dritte Ebene Nummer 1 ▪ Dritte Ebene Nummer 2 ▪ Dritte Ebene Nummer 3 3. **Überschrift zweiter Ebene** 4. **Überschrift zweiter Ebene** 3. **Überschrift erster Ebene** 4. **Und die letzte Überschrift**	1. **Inhaltsverzeichnis** 2. **Überschrift erster Ebene** 1. Überschrift zweiter Ebene 2. Überschrift zweiter Ebene Dritte Ebene Nummer 1 Dritte Ebene Nummer 2 Dritte Ebene Nummer 3 3. **Überschrift zweiter Ebene** 4. **Überschrift zweiter Ebene** 3. **Überschrift erster Ebene** 4. **Und die letzte Überschrift**

Unter den Dienstleistern, die barrierefreie PDF-Dokumente erstellen, herrscht allerdings Unmut über den BITV-Test. „Weg mit der PDF-Prüfung im BITV-Test“, fordert Brigitte Bornemann-Jeske von der BIT GmbH. Die PDF-Prüfung solle nicht zum Pflichtprogramm des Tests gehören. Nach wie vor sei die Technik unausgereift, weswegen barrierefreie PDF-Dokumente nicht zu den Standardanforderungen an barrierefreie Webseiten gehören sollten. Bornemann-Jeske weist zudem darauf hin, dass die aktuelle Regelung zu unstrukturierten Handlungen führt: „PDF-Dokumente werden mit großem Aufwand „nachgetaggt“, bei miserabler technischer Unterstützung.“ Wichtiger sei es, dass man Druck auf den Softwarehersteller Adobe ausübe, der für die technische Misere verantwortlich zeichnet.

Aufwand für das Erfüllen von Kriterien

Zu den wenigen Dokumentationen gehört Adobes Publikation „Erstellen von barrierefreien PDF-Dokumenten mit Adobe Acrobat 7.0“. Sie ist umfangreich und punktuell hilfreich, stammt allerdings schon aus dem Jahr 2005 und lässt viele Fragen offen. Bis heute gibt es keine aktuellere Version dieses Dokuments – im Gegenteil: Zu finden ist es im „Accessibilty Design Center“ von Adobe, wo der Hersteller den drei Jahre alten Text an populärer Position bewirbt. Immerhin ist eine neue Version für die kommenden Wochen angekündigt. Die „Beispiele für barrierefreie Inhalte“ auf der Website enthalten leider nicht ein einziges PDF. Bedenklich ist, dass die Dokumentation „Lesen von barrierefreien PDF-Dokumenten mit Adobe Acrobat 7.0“ (Handbuch für Benutzer mit Behinderungen) bei einer Prüfung auf Basis der vom Hersteller selbst aufgestellten Kriterien durchfallen würde.

Bleibt die Frage, wie sich bei der Erstellung barrierefreier PDF-Dokumente ein vernünftiges Resultat erzielen lässt, das den BITV-Test erfüllt, die automatische Prüfung fehlerfrei meistert und das wichtigste Kriterium erfüllt: die Zugänglichkeit zumindest zu erleichtern. Eine zu hundert Prozent gültige Antwort hierauf gibt es derzeit nicht, jedoch werden im Folgenden Ansätze beschrieben, wie man diesem Ziel nahekommen kann.

Zunächst gilt es zwischen zwei Dokumententypen zu unterscheiden: Cross-Media-Dokumenten, die sowohl als Print- als auch als Onlinedokument erscheinen, sowie reinen Onlineveröffentlichungen. Erstere erstellen Autoren beispielsweise mit QuarkXpress, TeX oder Adobes Indesign. Dabei gewährleistet nur die Verwendung von Indesign bei der richtigen Vorbereitung der Texte ein bezüglich der Barrierefreiheit vernünftiges Resultat.

Eine Nachbearbeitung in Acrobat ist zumeist erforderlich. Anwender haben hierzu einerseits die Möglichkeit, einen Tag-Stamm automatisiert zu erstellen. Für Cross-Media-Dokumente kommt innerhalb von Acrobat nur die Funktion „Tags zum Dokument hinzufügen“ infrage, die versucht, automatisch Elemente zu identifizieren und zuzuordnen. Das Resultat ist ernüchternd, und eine händische Auszeichnung des gesamten Dokuments erscheint zumeist schneller als die automatisch erzeugten Tags korrekt zu sortieren und umzudefinieren. Fragt sich, wieso die automatische Erstellung des Tag-Stamms in Acrobat so schlechte Resultate liefert. Laut Hersteller kann die Software bei einer automatisierten Erstellung „nicht immer zwischen instruktiven Abbildungen und dekorativen Seitenelementen“ unterscheiden. Weitere Schwierigkeiten ergeben sich durch Grafikzeichen im Text. Solche Fehler können dazu führen, dass der Tag-Baum unübersichtlich und die Lesereihenfolge für die Hilfstechnik zu kompliziert wird.

Gute Resultate durch gute Vorbereitung

Bei Dokumenten, die der Anwender in Textverarbeitungsprogrammen wie Microsofts Word oder der Open-Source-Software Openoffice erstellt, kann er bei guter Vorbereitung vernünftige Resultate erzielen – von einigen wenigen Fehlern und einem geringen Bedarf an manueller Nachbearbeitung abgesehen. Openoffice liefert die Funktion zur Erstellung von PDF-Dokumenten direkt mit, bei Word muss man ein Konvertierungs-Plug-in installieren. Folgende Punkte gilt es bei der Vorbereitung von Word-Dokumenten zu beachten:
– Speziell bei Überschriften sollten Formatvorlagen zum Einsatz kommen.
– Alternativtexte sollte der Autor bereits in der Textverarbeitung vergeben.
– URLs sollten als konkrete Hyperlinks ausgezeichnet sein.

Innerhalb von Openoffice gelten dieselben Regeln, deren Anwendung über vergleichbare Dialoge erfolgt.

iX-TRACT

- Barrierefreie PDF-Dateien sollen den Inhalt von Dokumenten auch Menschen mit körperlichen Einschränkungen zugänglich machen.
- Damit dies möglich ist, können Autoren Dokumente mit speziellen Tags versehen. Unterstützung dafür bieten die Produkte Acrobat und Indesign von Adobe.
- Die Technik, die die Erstellung barrierefreier PDF-Dokumente unterstützt, lässt noch zu wünschen übrig und garantiert nicht, dass ein Dokument den Test der „Barrierefreien Informationstechnik-Verordnung“ erfolgreich durchläuft.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Zusätzlich muss der Autor in Word darauf achten, dass bei den Konvertierungseinstellungen die Haken bei „Textzugriff für Sprachausgabeprogramme für Sehbehinderte“ und „Erweiterte Tag-Erstellung aktivieren“ gesetzt sind. Zusätzlich kann er unter der Registerkarte „Lesezeichen“ einstellen, dass Word die Überschriften direkt in Lesezeichen konvertiert. Openoffice-Anwender müssen sicherstellen, dass innerhalb der PDF-Optionen der Haken bei „Tagged PDF“ gesetzt ist.

Beiden Arten von Dokumenten – Cross-Media- sowie speziell für die Onlinepublikation erstellten PDFs – fehlen aber mitunter bestimmte Eigenschaften, um die BITV-Kriterien zu erfüllen oder der Prüfung in Acrobat zu genügen.

Manuelle Bearbeitung kann optimieren

Die folgenden Beschreibungen sind ein Versuch, die existierenden Anforderungen und Spezifikationen so zusammenzuführen, dass ein optimales Resultat entsteht. Hierbei ist die sorgsame Verwendung von Tags unerlässlich. Manuell lassen sich die Tags nur in Adobes Acrobat ab der Professional-Version mit dem Touch-Up-Leserichtungswerkzeug erzeugen.

Eine der wenigen Maßnahmen, um die Bearbeitung zu vereinfachen, ist die Identifizierung von Hintergrundelementen, die nicht in den Tag-Stamm aufgenommen werden. Hierzu gehören meistens Kopf- und Fußzeilen, Schmuckbilder sowie Listenpunkte, beispielsweise Spiegelstriche.

Des Weiteren muss der Autor die grundsätzliche Entscheidung treffen, ob er einen hierarchischen oder einen nichthierarchischen Tag-Stamm verwenden will. Hierarchisch bedeutet, logische Blöcke eines Dokuments in Containerelemente wie Kapitel (*<div>*) und Abschnitt (*<sect>*) zu trennen. Bei einem nichthierarchischen Aufbau erfolgt die Anordnung aller Tag-Elemente auf einer Ebene. Unter BIK-Kriterien ist hinsichtlich dieser Frage lediglich zu beachten, dass ein Dokument eine hierarchische Überschriftenstruktur enthält, sofern eine solche Struktur erkennbar ist. Ein Ansatz zur Einordnung wäre, dass in kurzen Dokumenten eine nichthierarchische Struktur vertretbar, ansonsten aber die aufwendigere Lösung mit hierarchischer Komposition vorzuziehen ist.

Mit wenig Aufwand lässt sich ein geeigneter Weg finden, Absätze mit Fließtext und Überschriften innerhalb von Kapiteln aufzubauen. Textdokumente enthalten jedoch einige klassische Elemente, bei denen die PDF-Tag-Technik an ihre Grenzen stößt. Dazu gehören Listen, Inhaltsverzeichnisse, komplexe Tabellen sowie mehrsprachige und mehrspaltige Dokumente. Eine mit Tags versehene Beispieldatei mit allen genannten Elementen ist über den *iX*-FTP-Server erhältlich.

Wer Listen mit Tags versehen will, muss sich zunächst entscheiden, ob er die Listenzeichen als Hintergrundelemente behandeln will oder ob sie eine inhaltliche Bedeutung haben sollen (siehe oben). Die gesamte Liste muss innerhalb des Behälterelements *<l>* stehen (Abbildung 2). Jeder einzelne Punkt ist eine Konstruktion aus umschließenden Element (*<li>*) sowie dem darin enthaltenen Körper (*<lbody>*) mit dem Inhalt. Optional – dies ist der Fall, wenn die Listenpunkte beispielsweise numerische Aufzählungen sind, – gehört in das Listenelement die Beschriftung (*<lbl>*), in dem sich der Listenpunkt befindet.

Derzeit kann man keine klare Aussage darüber treffen, ob und wie sich ein Inhaltsverzeichnis mit Tags versehen lässt. Ein Argument spricht dafür, es überhaupt nicht auszuzeichnen und es damit als Hintergrundelement zu behandeln, da Lesezeichen das Inhaltsverzeichnis adäquat ersetzen. Der BITV-Test unterstützt diese These: Sofern das PDF-Dokument auf Basis der Lesezeichen navigierbar ist, gilt dies als positiv.

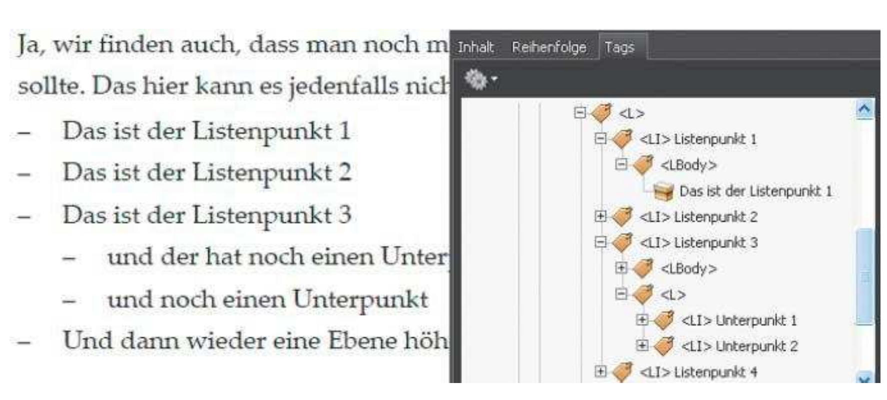


Die Tag-Reihenfolge in Flyern sollte sich an der tatsächlichen Reihenfolge im gefalteten Dokument orientieren, was über die Verwendung von Behälterelementen einfach realisierbar ist (Abb. 3).

Acrobat stellt aber auch spezielle Tags für Inhaltsverzeichnisse zur Verfügung: Table of Content (*<toc>*) als Behälterelement sowie Table of Content Item (*<toci>*) für die einzelnen Einträge. Diese Tags genügen jedoch nicht, wenn die Tags äquivalent zu den HTML-Auszeichnungen sein sollen. Da Inhaltsverzeichnisse eine Auflistung der Überschriften repräsentieren, benötigt der Anwender Listen-Tags, was ein Inhaltsverzeichnis rasch zu einem umfangreichen Tag-Gebilde werden lässt.

Komplexe Tabellen sind schwer erfassbar

Bereits bei der Erstellung von Tabellen muss der Autor Wert darauf legen, dass der Inhalt für Screenreader logisch erfassbar ist. Dies bedeutet zum Beispiel, keine einzelnen Zellen miteinander zu verbinden oder Überschriftenzellen für mehrere Spalten oder Zeilen zu konzipieren. Viele Tabellenkonstruktionen, die mit XHTML W3C-konform realisierbar sind, lassen sich mit den PDF-Tags nicht abbilden.



Der zur Liste im PDF (links) gehörige hierarchische Tag-Baum (rechts) muss innerhalb des Behälterelements *<L>* stehen (Abb. 2).

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Die in der Beispieldatei enthaltene Tabelle ist eine Referenz dafür, dass verschachtelte komplexe Tabellen mit dem Tag-Satz nicht erfassbar sind. Denn es stehen nur Tags für die Tabelle selbst (*<table>*), Zeilen (*<tr>*), Überschriftenzellen (*<th>*) und Datenzellen (*<td>*) bereit. Einzelne Zellen innerhalb einer Spalte lassen sich nicht miteinander verbinden. Es kann eine Hilfe sein, eine Tabelle in mehrere Tabellen zu unterteilen und diese zusammen in eine Gesamttabelle einzuordnen.

Es ist auch möglich, Tags zu integrieren, die lediglich Informationen für Screenreader liefern sollen, aber keinem Inhaltselement im PDF zugeordnet sind. Mit diesen unsichtbaren Elementen lässt sich eine Tabelle ohne Überschriftenzeile mit einer unsichtbaren Hilfe versehen. Der PDF-Standard fordert jedoch, dass jeder Tag einem tatsächlichen Inhalt zugeordnet ist. Diese Vorgabe kann mitunter zu Kollisionen bei der automatischen Prüfung führen.

Innerhalb barrierefreier PDF-Dokumente muss eine Hauptsprache definiert sein. Vereinzelt werden jedoch Dokumente veröffentlicht, in denen zwei Sprachen quasi gleichwertig dokumentenweit nebeneinander stehen. Unter den Kriterien der Barrierefreiheit müsste der Autor trotzdem eine Hauptsprache vergeben. Die nicht als solche definierte zweite Sprache wird dann in allen Inhalten im jeweiligen Tag angegeben.

Im Umfließen-Modus verursachen vor allem mehrspaltige Dokumente Schwierigkeiten. Das liegt allerdings in den meisten Fällen nicht an einer fehlerhaften Auszeichnung der Inhalte, sondern an der falschen Funktionsweise dieses Darstellungsmodus in Acrobat. Die Beispieldatei erreicht bei der automatischen Prüfung den Status, fehlerfrei zu sein. Im Umfließen-Modus wird allerdings die zweite Seite überhaupt nicht verändert, und in der Tabelle auf der dritten Seite überlappen sich die Inhalte.

Flyer lassen sich korrekt auszeichnen

Öffentliche Anbieter geben häufig Flyer heraus, die innerhalb eines PDF-Dokuments aus zwei Seiten bestehen. Die Lesereihenfolge ist aber eine andere, da nach dem Zusammenfalten mindestens sechs Seiten entstehen. Ein Beispiel hierfür ist der Flyer „Artenschutz im Urlaub“, herausgegeben vom Bundesministerium der Finanzen. Hier darf die Auszeichnung der Tags nicht von links oben nach rechts unten erfolgen, sondern das rechte Drittel der Seite 1 ist das erste Element, gefolgt von der Seite 2 von links nach rechts sowie der Seite 1 von links bis zur Mitte. Screenreader lesen den Inhalt durch diese Vorgehensweise korrekt vor (Abbildung 3).

Neben den erwähnten Schwachpunkten der Auszeichnungstechnik erschweren einige andere Aspekte die Arbeit mit Acrobat, wenn es darum geht, barrierefreie Dokumente zu erstellen:

– Schließt der Anwender ein Dokument während der Tag-Bearbeitung, erscheint keine Sicherheitsabfrage, ob er die Änderungen speichern möchte.
– Bei einer Speicherung klappen alle Behälterelemente im Tag-Stamm zu, und der Anwender muss sie zur Weiterbearbeitung neu öffnen.
– Die Bezeichnungen der Tags in der Adobe-Dokumentation weichen von denen im Programm ab.
– Bei der Bearbeitung mit dem Touch-Up-Leserichtungswerkzeug steht nur ein Teil der benötigten Tags zur Verfügung.
– Die Bezeichnungen der Tags in der deutschen Version sind übersetzt, sodass der jedem Internetentwickler geläufige Tag *<div>* unter dem Begriff „Teilung“ zu finden ist.
– Änderungen im Dialogfenster „Touch-Up-Eigenschaften“ wurden bis zur Version 9 erst übernommen, nachdem der Anwender das geänderte Eingabefeld verlassen und das Fenster geschlossen hatte.
– Es ist häufig der Fall, dass beim Auszeichnen mit Tags Inhalte aus dem sichtbaren Bereich verschwinden. Dies liegt vermutlich daran, dass sich die Hierarchie der Ebenen beim Auszeichnen dokumentintern ändert. Abhilfe schafft in dem Fall nur der Weg über das Navigationsfenster „Inhalte“. Der „verschwundene“ Inhalt kann hier wiedergefunden und durch eine Verschiebung in der Hierarchie erneut sichtbar gemacht werden.

Acrobat 9 hilft auch nicht weiter

Im Juni 2008 ist die Version 9 von Adobes Acrobat erschienen. Bezüglich der in diesem Artikel betrachteten Eigenschaften und Funktionen gibt es so gut wie keine Veränderung. Die erwähnten Schwachstellen und Barrieren sind erhalten geblieben. Das bedeutet, die bis mindestens zur nächsten Release zu verwendende Technik ist bereits drei Jahre alt. Zu beachten ist, dass Adobe mit Acrobat 9 die neue Version Pro Extended eingeführt hat, in der Anwender Videos und PDF-Karten einbetten können. Diese neuen Elemente kann der Anwender laut Hersteller mit Tags versehen. (ka)

Onlinequellen

Barrierefreie Informationstechnik-Verordnung (BITV)
de.wikipedia.org/wiki/BITV

Barrierefrei Informieren und Kommunizieren (BIK)
www.bik-online.info

Presseerklärung zur Umsetzung des Behindertengleichstellungsgesetzes
www.bik-online.info/test/ministerien_2006/pressemitteilung.php

BITV-Test
bitvtest.de

Anforderungen des BITV-Tests an PDF-Dokumente
www.bitvtest.de/index.php?a=di&iid=1125&s=n

Creating Accessible PDF Documents with Adobe Acrobat 7.0
www.adobe.com/enterprise/accessibility/pdfs/acro7_pg_ue.pdf

Accessibility Design Center
www.adobe.com/de/accessibility/

Flyer „Artenschutz im Urlaub“
www.bundesfinanzministerium.de/nn_618/DE/BMF__Startseite/Service/Broschueren__Bestellservice/Zoll/60404,templateId=raw,property=publicationFile.pdf

HELMUT MORITZ

arbeitet als Produktmanager bei der 1&1 Internet AG.

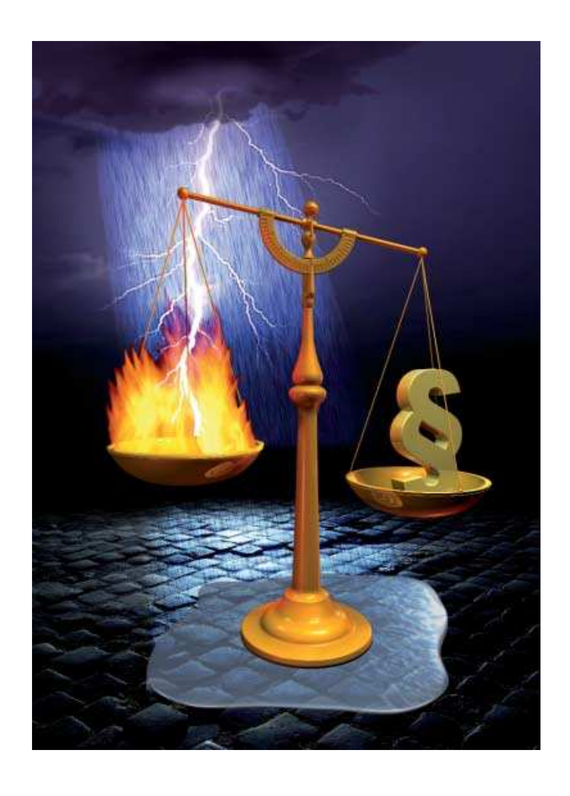




© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Höhere Gewalt in Verträgen berücksichtigen

Unvorhersehbar

Tobias Haar

Wenn in der heutigen vernetzten Welt kritische Geräte oder Dienste ausfallen, kann es teuer werden – auch wenn es wegen „höherer Gewalt“ passiert. Wer solchen Szenarien durch rechtliche Voraussicht begegnet, ist auf der sicheren Seite.

Als Anfang 2008 innerhalb weniger Tage von insgesamt vier Seekabel-Brüchen im Mittelmeer und im Persischen Golf die Rede war, machten sogleich Verschwörungstheorien die Runde. Sie stellten sich später als haltlos heraus. Für jeden Kabelbruch gab es eine plausible Erklärung: Schiffsanker hatten die beiden Kabel vor der ägyptischen Küste und eines im Persischen Golf zerrissen. Ein Stromausfall beschädigte ein weiteres Kabel im Persischen Golf. Letztlich blieb auch das befürchtete Chaos aus. Immerhin verlor das für die Call-Center-Industrie wichtige Ägypten vorübergehend etwa 70 Prozent seiner Internet-Kapazität und 30 Prozent der internationalen Telefonverbindungen. Nach Angaben der Firma FLAG, die zwei dieser Seekabel betreibt, waren 85 Millionen Internetnutzer vorübergehend offline.

Mittlerweile haben Spezialfirmen die Schäden an den Kabeln beseitigt, doch einige Fragen bleiben. Etliche IT-Abteilungen von Unternehmen lassen mögliche Ansprüche gegen ihre Telekommunikationsanbieter prüfen, weil beispielsweise die Niederlassung oder der Outsourcing-Dienstleister in Indien keinen oder spürbar gebremsten Zugriff auf die Unternehmensnetze hatte. Die Dienstleister erteilen dann meist eine Absage und verweisen auf „höhere Gewalt“, für die man eben nicht einzustehen habe. Das ist rechtlich betrachtet richtig und falsch zugleich.

Gerade unternehmenskritische Prozesse erfordern juristische Überlegungen zur Festlegung des Handlungsbedarfs, damit man im Fall der Fälle nicht „ohne Netz“ dasteht. IT-Verantwortliche, die hier falsche Entscheidungen treffen oder zu lax handeln, bringen nicht nur ihre Firma in Gefahr, sondern – weil sie vielleicht bestimmte allgemeingültige Standards missachten – auch ihren Arbeitsplatz. Organe wie Vorstände von Aktiengesellschaften fangen sich zudem auch Regressansprüche der Gesellschaft ein.

Im Gesetz nicht vorgesehen

Wer viel mit Verträgen zu tun hat, kommt früher oder später mit Klauseln zu „höherer Gewalt“ oder „force majeure“ in Berührung. Gerade in angloamerikanischen Verträgen gehören sie – genau wie Klauseln zur Haftung, zum anwendbaren Recht oder zum Gerichtsstand – an sich zu den Standardregelungen, die in keinem Vertrag fehlen dürfen. In deutschen oder kontinentaleuropäischen Verträgen hingegen sind sie weniger verbreitet, weil sie streng genommen – etwa nach deutschem Recht – nicht zwingend erforderlich sind. Allerdings nehmen auch deutsche Juristen immer häufiger solche Klauseln in unternehmenskritische Verträge auf.

Dahinter steht zum einen, dass man sich im internationalen Geschäftsverkehr mittlerweile häufig an Gepflogenheiten im US-amerikanischen Recht orientiert. Tendenziell vereinheitlicht sich „die“ internationale Vertragssprache, und regionale Besonderheiten verblassen. Zum anderen – und das ist aus rechtlicher Sicht ein valides Argument – verlässt man sich dann nicht mehr auf das, was sowieso im Gesetz steht, sondern regelt für beide Vertragspartner in (hoffentlich) eindeutiger Weise, was für sie unter dem Begriff „höhere Gewalt“ zu verstehen ist und – fast noch wichtiger – was gelten soll, wenn ein solcher Fall tatsächlich eintritt. Gerade die Seekabel-Fälle zeigen, dass solche Situationen viel häufiger eintreten, als man meinen möchte.

Mit äußerster Sorgfalt

Eine Definition des Begriffs „höhere Gewalt“ gibt es im deutschen Recht nicht. Das Bürgerliche Gesetzbuch (BGB) nennt es „Zufall“ (§ 287 BGB) oder „zufälligen Untergang“ (§ 848 BGB), wenn jemand für den Verlust einer Sache auch dann einzustehen hat, falls ihn an dem Verlorengehen gar keine „Schuld“ trifft. Eine Definition könnte aber lauten, dass es sich

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

bei höherer Gewalt um „ein von außen kommendes, außergewöhnliches und unvorhersehbares Ereignis handelt, das auch äußerste Sorgfalt des Betroffenen nicht verhindern kann". Es muss sich also um einen Umstand handeln, den der Betroffene nicht beeinflussen kann. Als typische Fälle von höherer Gewalt gelten landläufig Brand, Unwetter, Erdbeben, Streiks, Unfälle, Krieg, Unruhen, Naturkatastrophen et cetera. In der englischen Vertragssprache werden häufig die anschaulichen Begriffe „Act of Nature" oder „Act of God" verwendet.

Letztlich geht es also darum, wer für eine nicht vertragsgemäß erbrachte Leistung einzustehen hat. Dabei geht es häufig um viel Geld. Wenn eine unternehmenskritische IT-Anwendung für mehrere Stunden nicht zur Verfügung steht, kann dies bedeutende Schäden verursachen. Der Auftraggeber oder Kunde eines Netzbetreibers wird sich dann die Frage stellen, ob er seinen TK-Anbieter für den Ausfall einer Leitung und den Ersatz des dadurch verursachten Schadens heranziehen kann. Das kann er in den Fällen von „höherer Gewalt" allerdings nicht. Denn es ist für den TK-Anbieter eben nicht beherrschbar und nicht vorhersehbar, dass ein Schiff ein Seekabel durchtrennt.

Oder vielleicht doch? Damit muss man doch rechnen, wenn man sich vor Augen hält, wie häufig solche Kabelbrüche vorkommen. Daher sind TK-Anbieter an sich auch verpflichtet, Redundanzen zu schaffen und alternative Routen für ihre Datenströme vorzuhalten. Das tun sie auch. Durch Absprachen mit Staaten stellen sie – wie im Fall der Seekabel nach Ägypten – sicher, dass sich in der kritischen Zone des Übergangs des Kabels vom Meer in ein Land keine Schiffe aufhalten dürfen und treffen weitere wirksame Schutzmaßnahmen. All diese Vorkehrungen gab es im Fall der betroffenen Seekabel. Der Seekabel-Betreiber hat also mit „äußerster Sorgfalt" gehandelt, und deswegen kann ihm niemand den Bruch des Kabels vorwerfen. Für ihn war der zeitlich begrenzte Ausfall bestimmter Übertragungskapazitäten auf „höhere Gewalt" zurückzuführen.

Auch der Kunde muss sich – eventuell nach entsprechendem Hinweis durch seinen TK-Anbieter – die Frage stellen, ob er für solche Fälle Backup-Möglichkeiten bereithalten muss. Denn es kann rechtlich auch nicht angehen, dass sich ein Kunde für die billigste aller Lösungen entscheidet mit der Einstellung, dass im schlimmsten Fall ohnehin der TK-Anbieter für den Schaden einzustehen hat, wenn er einmal nicht „äußerste Sorgfalt" walten ließ. TK-Anbieter sind letztlich keine Versicherungen, sondern „nur" zur Erfüllung der vertraglich vereinbarten Leistung verpflichtet. Grundsätzlich versuchen sie auch, ihre Haftung für Fälle des Netzausfalls oder einer Störung zu begrenzen oder ganz auszuschließen.

Im Einzelfall ist die Abgrenzung der Aufgaben und Verantwortlichkeiten zwischen Kunde und Anbieter also schwierig. Daher gilt – wie so oft – der Grundsatz: Wer schreibt, der bleibt. Wer in einem Vertrag die Grenzen der eigenen Verantwortung gerade für solche „Krisenfälle" ausführlich und eindeutig beschreibt, bleibt vor juristischem Ärger gefeit. Wichtig sind auch Regelungen über die Verfügbarkeit und etwaige Reaktionen im Fall eines Netzausfalls. Soll der Anbieter zusätzliche Redundanzen aufbauen? Welche Eskalation soll erfolgen? Welche Anbindungen haben Vorrang vor anderen, wenn Kapazitäten nur eingeschränkt verfügbar sind?

Höhere Gewalt hat ihre Grenzen

Auch die Reichweite dessen, was als „höhere Gewalt" gilt, sollte der Vertrag im Zweifel genau beschreiben. Sind Streiks selbst mit „äußerster Sorgfalt" nicht zu vermeiden? Was, wenn es sich um eine rechtswidrige „Arbeitskampfmaßnahme" des Arbeitgebers handelt, zum Beispiel eine Aussperrung, und deswegen bestimmte Dienstleistungen nicht mehr zur Verfügung stehen? Dann hat an sich der Arbeitgeber – der Dienstleister eines Kunden – die Unmöglichkeit der Leistungserbringung selbst herbeigeführt und kann sich nicht auf „höhere Gewalt" berufen, auch wenn Arbeitskampfmaßnahmen landläufig dazu zählen.

Die Grundsätze zur höheren Gewalt gelten für sämtliche vertraglichen Ansprüche. Bei Unterschreiten einer vertraglich vereinbarten Dienstqualität (Service Level) aufgrund höherer Gewalt sind Vertragsstrafen oder „Credits" in der Regel ausgeschlossen. Es sei denn, der Anbieter hat den Fehler gemacht, die Einhaltung bestimmter Performance-Kriterien zu garantieren. Dann hat er die Verantwortung dafür übernommen, dass die Leistung diesen Vorgaben entspricht – egal, ob er etwa einen Netzausfall zu vertreten hat oder nicht.

Für die Internetprovider bedeutete der Verlust von Leitungen im Mittelmeer und im Persischen Golf, dass die Westanbindung massiv gestört war und der Datenverkehr beispielsweise von dort einen Umweg über Ostasien, die Vereinigten Staaten und über den Atlantik nach Europa nehmen musste. Dies bremste zwangsläufig die Übertragung, aber immerhin ließ sich die Kommunikation aufrechterhalten. Dieses Beispiel zeigt die Voraussicht der Telekommunikationsanbieter. Denn nur weil sie sich für solche Fälle Backup-Bandbreite gesichert hatten, konnten sie schnell reagieren und eben diese Alternativen anbieten. Zudem zeigt dieses Beispiel, welche Einkaufsstrategie Unternehmen verfolgen müssen, die besonders auf Erreichbarkeit ihrer ausgelagerten Systeme und Abteilungen angewiesen sind. Die Stichworte lauten „Redundanz" und „Diversifikation".

Fazit

Kommt es bei unternehmenskritischen Prozessen auf Leistungen von Dritten an, beispielsweise auf Netzwerk- oder Datenzentrumskapazität, dürfen die Vertragspartner nicht nur die typischen Themen wie Haftung, Service Level et cetera im Auge haben. Sie müssen sich mit allen möglichen Unwägbarkeiten der Vertragserfüllung befassen. Dazu zählt auch, sich mit Fällen der „höheren Gewalt" auseinanderzusetzen.

Sich hier ganz und gar auf die gesetzlichen Vorschriften zu verlassen, reicht meist nicht aus. Denn sie beschreiben nicht, welche Anstrengungen ein TK-Anbieter beispielsweise unternehmen muss, wenn ein kritisches Seekabel ausfällt. Wer vorausschauend handelt und bei der Vertragsgestaltung aufpasst, schützt nicht nur das eigene Unternehmen, sondern auch seinen eigenen Arbeitsplatz. Wer grob fahrlässig das eigene Unternehmen – also meist den Arbeitgeber – hohen Risiken aussetzt, kann wegen Verletzung des Arbeitsvertrages sogar den Job verlieren. (un)

TOBIAS HAAR, LL.M.,

ist Rechtsanwalt mit Schwerpunkt IT-Recht.



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

25 Jahre Domain Name System

Nachschlagewerk

Christian J. Dietrich



Das Domain Name System bildet seit einem Vierteljahrhundert einen Grundbaustein des Internet. Seine ursprüngliche Aufgabe – die Zuordnung von Domänen und Host-Namen zu IP-Adressen – erfüllt das 1983 von Paul Mockapetris entworfene DNS bis heute, und einige darüber hinaus.

Als vor 25 Jahren die RFCs 882 und 883 erschienen, waren längst nicht alle Aufgaben absehbar, die das DNS heute erledigt, etwa das Abfragen von IP-Adress-Blacklists über DNS zur Spam-Abwehr oder die Auflösung von Telefonnummern (ENUM). Nach wie vor ist jedoch die Namensauflösung seine wichtigste und unverzichtbare Aufgabe. Ein längerer Ausfall des DNS hätte sicherlich einen großflächigen Zusammenbruch von Diensten im Internet zur Folge, denn wer kennt schon die IP-Adressen diverser Webseiten oder anderer Dienste im Internet auswendig?

Bereits bevor DNS erfunden war, hatte es sich eingebürgert, anstelle der eindeutigen, aber für Menschen schwer erinnerbaren IP-Adressen Aliase, sogenannte Host-Namen zu verwenden. Die „Übersetzung“ eines Host-Namens in eine IP-Adresse fand lokal auf jedem Computer mithilfe der Datei *hosts* statt, einer einfachen Liste. Das Domain Name System entstand in erster Linie aus der Notwendigkeit, diese manuell gepflegten Tabellen zur Namensauflösung auf allen ans Internet angeschlossenen Computern durch ein verteiltes System abzulösen. Die Fehleranfälligkeit sowie die mangelnde Flexibilität der manuell gepflegten Dateien stieg mit der Zahl angeschlossener Computer.

Das DNS war daher von vornherein als verteiltes System konzipiert, dessen Datenbestand auf vielen verschiedenen zuständigen Servern lag. Der komplette DNS-Namensraum liegt also nicht an einer zentralen Stelle vor, sondern ergibt sich durch die Menge aller verteilten Domain-Datenbanken, die sogenannten Zonen. Auf dem für eine Domain verantwortlichen („autoritativen“) Nameserver wird daher in der Regel nur die entsprechende Zone angepasst. Ein weiterer Vorteil dieses Mechanismus ist die erhöhte Ausfallsicherheit mittels Datenverteilung.

Der DNS-Namensraum hat die mittlerweile in RFC 1034 definierte fest vorgegebene Struktur. Ein absoluter Name gliedert sich in „Labels“, die durch Punkte voneinander getrennt sind. Die Wurzel des DNS bildet die „nameless root“. Korrekterweise müsste jeder DNS-Name mit einem Punkt enden, doch nur sehr selten findet er sich am rechten Ende eines Domainnamens. In der Regel lässt man ihn einfach weg. Unterhalb der Wurzel befinden sich die „Top-Level-Domains“, kurz TLDs. Es gibt über 200 länderspezifische TLDs wie .de, .fr oder .at und die generischen TLDs wie .com, .org oder .net. Die Vergabe von Sub-Domains innerhalb einer TLD geschieht sehr unterschiedlich. Die Registry Denic ist verantwortlich für die TLD .de und verlangt vom Inhaber einer .de-Domain einen Wohnsitz in Deutschland.

Im Kontrast dazu vermarkten andere Nationen ihre TLD in der Hoffnung auf hohe Registrierungseinnahmen ohne derartige Restriktionen, etwa der Staat Tuvalu seine TLD .tv, die viele mit „Fernsehen“ assoziieren. Auch wenn kleine Inselstaaten im Internet sonst keinen allzu guten Ruf haben, nutzt manch eine Aktiengesellschaft die TLD .ag (von Antigua und Barbuda) für sich und mancher Radiosender .fm (für Mikronesien) in Anlehnung an das analoge Sendeverfahren der Frequenzmodulation. Unterhalb der Top-Level-Domains befinden sich Second-Level-Domains wie heise.de, darunter Third-Level-Domains wie www.heise.de und so weiter.

Die Welt der Domainnamen ist immer wieder für Anekdoten und Kuriositäten gut. So geriet im August 2004

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

die Domain ebay.de vorübergehend in die Hände eines Dritten, sodass die Auktionsplattform für einige Internetnutzer zeitweise scheinbar nicht erreichbar war – zumindest eben nicht über diesen Namen. Auf ähnliche Weise ereilte es google.de im Januar 2007.

Neben technischen und organisatorischen Pannen bieten Domains ein weitläufiges Spielfeld für juristische Auseinandersetzungen. Einer der aktuelleren Fälle ist der Streit zwischen dem Rohrunternehmen Universal Tube mit der Domain utube.com und dem Videoportal youtube.com um die Namensähnlichkeit. Den Rohrkonzern ärgerte das unerwünscht hohe Besuchsaufkommen durch Benutzer, die eigentlich das Videoportal aufsuchen wollten. Darüber hinaus gibt und gab es zahlreiche Auseinandersetzungen um Domains, die von mehreren Parteien gewünscht waren, so zwischen der Schokoladenmarke Milka und einer französischen Schneiderin Milka um die Domain milka.fr.

Des DNS-Rätsels Auflösung

Wie der Namensraum selbst ist auch der tatsächliche Prozess des Auflösens auf mehrere Systeme verteilt, denen dabei dreierlei Rollen zukommen – dem Anwender-PC in der Regel die des Clients. Der Rechner selbst führt keine DNS-Auflösung durch, sondern gibt die Aufgabe der Namensauflösung an einen „Resolver“ weiter. Der wiederum löst einen Namen im Zusammenspiel mit einem oder mehreren Nameservern auf. Wenn beispielsweise ein Browser eine Webseite vom Host www.internetsicherheit.de abrufen möchte, formuliert zunächst der Client eine Anfrage zur Namensauflösung an den Resolver. Der erfragt die entsprechende Antwort entweder iterativ oder rekursiv bei weiteren Nameservern und leitet die Antwort – in diesem Fall die IP-Adresse 194.94.127.43 – an den Client zurück. Aufgrund der strikt hierarchischen Struktur des Namensraums ergibt sich häufig eine ähnliche Reihenfolge für die Abfrage.

Den Startpunkt bei der Namensauflösung bildet häufig einer der 13 Root-Nameserver mit den Bezeichnungen A bis M. Sie sind weltweit verteilt und häufig besteht eine Instanz wiederum aus mehreren verteilten Rechnern. Sie enthalten in nur etwa 2500 Einträgen lediglich Verweise auf die Nameserver der Top-Level-Domains. Von hier aus hangelt sich der Resolver im Auflöseprozess bis zum aufzulösenden Namen Label für Label entlang.

Wurzelbehandlung

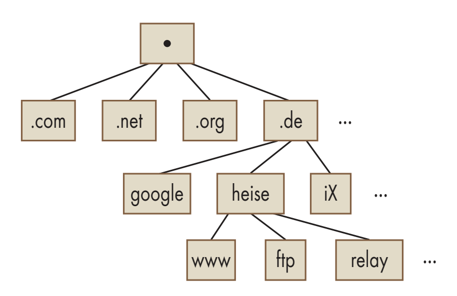
Die IP-Adressen der Root-Nameserver sind in der Regel fest in die DNS-Software einkodiert. Aus Perspektive der Sicherheit kommt den Root-Nameservern eine wichtige Rolle zu. Wer sie kapert oder die Auflösung auf andere Weise manipulieren kann, hat als Angreifer die Möglichkeit, Opfer gezielt auf andere Systeme zu leiten. Tatsächlich gab es einen solchen Fall im November 2007: Die IP-Adresse des L-Root-Nameservers änderte sich – ein zwar seltenes, aber umso gefährliche-res Phänomen. Die bis dahin gültige IP-Adresse ging in einen neuen Verantwortungsbereich und damit auch auf einen neuen Computer über. Nach einiger Zeit beantwortete der neue Computer wieder die noch immer eingehenden DNS-Anfragen.

Viele DNS-Server-Betreiber hatten diesen Wechsel wohl gar nicht bemerkt und nutzten so monatelang einen falschen Root-Nameserver. Der neue Computer hätte mit Leichtigkeit manipulierte Antworten einspielen können, was aber anscheinend glücklicherweise nicht passiert ist.

Schnell, unverbindlich und angreifbar

Die Betreiber der Root-Nameserver sind sich der Bedrohung seit Langem bewusst und beobachten häufig gezielte Denial-of-Service-Angriffe, die einzelne Root-Nameserver manchmal unerreichbar machten, etwa im Februar 2007. Endanwender bemerken jedoch selten Auswirkungen solcher Angriffe. Die Root-Nameserver sind so ausgelegt, dass zwei Drittel von ihnen ausfallen können, ohne dass die Namensauflösung darunter leidet – zumindest theoretisch.

Nicht nur Root-Nameserver sind ein Ansatzpunkt für Angriffe durch DNS-Spoofing, sondern auch die Namensauflösung im LAN oder gar auf dem Client. Zum Teil modifiziert Malware – darunter einige ZLOB-Varianten – die Namensauflösung auf dem infizierten Client und lockt das Opfer auf diese Weise unbemerkt auf eine schädliche Webseite, zum Beispiel zu Phishing-Zwecken.



Besonders die Domainnamen auf der zweiten Ebene unterhalb der durch einen Punkt symbolisierten Wurzel (Second-Level-Domains) sind immer wieder Anlass für Streitigkeiten zwischen Internet-Anwendern.

Das DNS-Protokoll baut in erster Linie auf dem User Datagram Protocol (UDP) auf, kommt also ohne zeit- und bandbreitenraubenden Verbindungsaufbau aus. Einerseits ermöglicht das die Implementierung von Resolvern in ressourcenarmen Umgebungen, die keinen vollständigen TCP-Stack erfordern, sondern lediglich IP und UDP. Andererseits bietet es weitere Angriffsflächen – in erster Linie wegen der Tatsache, dass auf eine kleine DNS-Anfrage mitunter große Antworten erfolgen („Amplification Attack“). Auf diese Weise können Angreifer den Datenverkehr im Rahmen eines Denial-of-Service-Angriffs um den Faktor 30 bis 50 verstärken. Fälscht man überdies die Absender-IP-Adresse, gelangen die großen Antwortpakete direkt zum Angriffsziel, ohne dass der tatsächliche Ursprung des Angriffs in Erscheinung tritt. Diese Technik kam bereits im Februar 2006 für einen Angriff auf Root-Nameserver zum Einsatz.

Weitere Angriffe auf DNS bestehen beispielsweise darin, gefälschte DNS-Antworten zu versenden, die den Cache eines DNS-Servers „vergiften“ (Cache Poisoning). Trotz der Vielfalt denkbarer Angriffe beweist das Domain Name System auf respektable Weise bis heute eine enorme Stabilität und skaliert trotz des enormen Internet-Wachstums reibungslos – vielleicht einer der Gründe dafür, dass sich Ansätze wie DNSSec, die die Sicherheit erhöhen sollen, noch nicht durchsetzen konnten. Bleibt an dieser Stelle nur eines zu sagen: Herzlichen Glückwunsch, DNS – und alles Gute für die Zukunft. (un)

CHRISTIAN J. DIETRICH

ist Mitarbeiter des Instituts für Internet-Sicherheit an der FH Gelsenkirchen und für den Forschungsbereich E-Mail-Sicherheit verantwortlich.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Strategien für ein energieeffizientes Data Center

Haushalten

Jana Behr

Auch wenn Green IT in der letzten Zeit zum Buzzword avancierte, ist es dennoch eines der bedeutenden IT-Themen der nächsten Jahre. Insbesondere für den Rechenzentrumsbetrieb lohnt es sich, über grüne Strategien nachzudenken. Einige Hersteller von Rechenzentrumskomponenten haben das auch schon getan – ein Überblick.

Die Zahlen sind eindeutig: Rund 25 % des IT-Energiebedarfs gehen auf das Konto von Rechenzentren – Tendenz steigend. Das ergab eine Analyse des IT-Marktforschungs- und Beratungsunternehmens Gartner. Nach der Studie „Zukunftsmarkt energieeffiziente Rechenzentren“ des Borderstep-Instituts im Auftrag des BMU hat sich der Energiebedarf deutscher Rechenzentren zwischen 2000 und 2006 auf rund 8,7 Milliarden Kilowattstunden mehr als verdoppelt, die Stromkosten haben sich aufgrund der gestiegenen Energiepreise sogar mehr als verdreifacht [1].

Dadurch bleibt für viele Rechenzentren der Energieverbrauch auch in den kommenden fünf Jahren einer der größten Kostenfaktoren, vor allem vor dem Hintergrund einer ständig steigenden Rechenleistung. 2010 sollen die Stromkosten laut der Branchenanalysten sogar bis zu 50 % des IT-Budgets ausmachen. Das Fraunhofer-Institut für System- und Innovationsforschung (ISI) erwartet in einer Studie von 2005 im Server-Bereich für den Zeitraum von 2001 bis 2010 eine Verdopplung des Stromverbrauchs [2]. Mit dieser steigenden Tendenz bewegt sich die IT-Branche, im Vergleich zu anderen, gegen den Trend.

Auch wenn der Klimaschutz das hehre Ziel beim Energiesparen ist, haben grüne Ansätze nur deshalb eine Chance, weil sie auch die Kasse der Unternehmen schonen. Allerdings gibt es tatsächlich so etwas wie ein ökologisch verträgliches Energiefenster. Das Schweizer Center for Energy Policy and Economics (CEPE) setzt dieses bei rund 17 500 kWh/Kopf im Jahr an [3]. Nahezu alle Industriestaaten liegen deutlich über diesem Wert, die USA und Kanada bei etwa dem Fünffachen und Deutschland bei etwa dem Doppelten. Einsparungen sind daher dringend geboten. Ein weiterer Grund zwingt einige Rechenzentren zur Umkehr in Sachen Energieverbrauch: Wenn die Leitungskapazität an ihre Grenze geraten ist, können die Energieversorger vielerorts keinen Ausbau gewährleisten. Deshalb bedeutet das Energiemanagement für Betreiber und Hersteller von Rechenzentren heute eine ökonomische, technische und ökologische Herausforderung.

Bevor man jedoch die Infrastruktur in Rechenzentren optimieren kann, steht man derzeit vor einer ganz anderen Hürde. So kennen nach einer aktuellen Umfrage der Marktforscher von Experton nur 7 % der deutschen

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

IT-Entscheider den Energiebedarf der eigenen IT.

Aber: Was man nicht messen kann, kann man auch nicht verbessern. Hier besteht großer Nachholbedarf. Der Grund dafür ist, dass in vielen IT-Budgets zwar die Etats für die Planung, Anschaffung und das Management der IT berücksichtigt sind, nicht aber die Energiekosten. Diese werden oftmals als allgemeiner Posten über das Facility-Management abgerechnet. Deshalb empfiehlt es sich, die Verantwortung für den Energieverbrauch der IT-Systeme dorthin zu legen, wo die Entscheidungen fallen: in die IT-Abteilung. Doch selbst wenn sie, etwa weil als eigenständige Tochter ausgegliedert, ihren Gesamtstromverbrauch kennt, sind die unnötigen Stromfresser noch längst nicht enttarnt.

Messen macht sich bezahlt

Manchmal reicht es, den Energiebedarf eines Rechenzentrums zu messen, um Potenziale zur Senkung des Verbrauchs und der Kosten aufzudecken. Zudem wirkt sich die Einbeziehung des Energieverbrauchs bei der Ausstattung eines Rechenzentrums auch auf Investitionsentscheidungen aus. Dadurch lässt sich beispielsweise einfacher darstellen, dass sich eine etwas höhere Investition in eine energieeffiziente Kühlung schon nach wenigen Monaten rentiert.

Für die Energieeffizienz eines Rechenzentrums gibt es eine Reihe von Kennzahlen (siehe Kasten „Kennzahlen zur Energieeffizienz“). Mit entsprechender Softwareunterstützung können diese Kennzahlen auch laufend berechnet und überwacht werden, um so weitere Potenziale zur Steigerung der Energieeffizienz zu erschließen.

Die Messungen von Energieverbrauch und Temperatur im Rechenzentrum können aber noch viel weiter gehen: Moderne Systeme ermöglichen es, detailliert den Energieverbrauch und die Temperaturverteilung im Rechenzentrum zu erfassen und zu visualisieren. Mit aktuellen Auditing-Methoden kann man anschaulich und in Echtzeit auf allen Ebenen den Energieverbrauch eines Rechenzentrums im Auge behalten – bis hinunter zu den einzelnen Komponenten.

Auch die Temperatur lässt sich zum Beispiel mit Infrarotkameras aufnehmen. Neben Momentaufnahmen sind aber kontinuierliche und flächendeckende Messungen sowie die Darstellung der historischen Entwicklung für das dauerhaft sichere und effizienzorientierte Betriebsmanagement erforderlich. Auf diesen Ergebnissen aufbauend lassen sich dann entsprechende Strategien entwickeln.

Die beschriebenen Entwicklungen führen zu großen Herausforderungen für Unternehmen bei der Planung und beim Betrieb ihrer Rechenzentren. Die Leistungsdichten dort haben sich in den letzten Jahren stark erhöht. Allein der durchschnittliche Pro-Rack-Energieverbrauch hat sich in den letzten drei Jahren verdreifacht. Rechenzentren mit einem Leistungsbedarf von 2500 Watt pro Quadratmeter und mehr sind keine Seltenheit.

Handeln ist gefordert

Fakt ist: Im Schnitt verbraucht die eigentliche IT nur die Hälfte der Energie eines Rechenzentrums. Die andere Hälfte benötigt die Infrastruktur wie Klimatisierung und unterbrechungsfreie Stromversorgung. Mit modernen Systemen lässt sich der Energiebedarf deutlich senken. Die Lösungsansätze der einzelnen Akteure sind recht unterschiedlich (siehe Kasten „Green-IT-Projekte der Big Five“). Neben anderen Maßnahmen wie Gebäude-Design, Green (Out)-Sourcing und der Nutzung erneuerbarer Energien kristallisieren sich zwei heraus: die Server-Konsolidierung durch Virtualisierung und energieeffiziente Kühllösungen.

Weithin bekannt ist, dass die durchschnittliche Serverauslastung nur 15 bis 30 % beträgt. Begründet hat man das bislang mit einer optimalen Performance während Lastspitzen und der nötigen Kapazität für den zukünftigen Ausbau. Außerdem soll das mögliche negative Auswirkungen im Fehlerfall begrenzen. Trotz nachvollziehbarer Motive lässt sich der signifikante Einfluss auf die Umwelt als Folge von ungenutzten Serverkapazitäten nicht von der Hand weisen.

Das Ergebnis ist eine teure und komplexe Hochverfügbarkeit mit ungenutzten und passiven Servern. Letztlich wird dieses Negativkonto noch um hohe operationale IT-Kosten, die Notwendigkeit individueller Backup-Jobs sowohl im Management als auch in puncto Lizenzen, dem Bedarf an Anti-Viren-Scans auf jedem Server, hohen

Kennzahlen zur Energieeffizienz

Green Grid (USA):

PUE (Power Usage Effectiveness):
Quotient aus Gesamt-Energieverbrauch und Energieverbrauch (nur) des IT-relevanten Inhaltes

DCE (Data Center Efficiency):
Quotient aus Energieverbrauch des IT-relevanten Inhalts und Gesamt-Energieverbrauch (= 1/PUE)

IEP (IT Equipment Power):
Verbrauch der Energie von IT-Verarbeitung, Speicherung und Verteilung plus Management

TFP (Total Facility Power):
Gesamt-Energieverbrauch inkl. der Energie von Klima (Kühlung), Stromlieferung, Überwachung, Beleuchtung etc.

Uptime-Instituts (USA):

SI-EER (Site Infrastructure-Energy Efficiency Ratio):
Verhältnis des Gesamtenergieverbrauchs zur Energie nur für die IT

IT-PEW (IT Productivity per Embedded Watt):
Wert, der die IT-Produktivität (Transaktionen, Speichermenge, Rechenzyklen) ins Verhältnis zur dafür benötigten Leistung setzt.

DC-EEP:
Produkt aus SI-EER und IT-PEW

Beispielrechnung PUE:

Beispiel: PUE = 2,5
1 kW Leistung für IT
= 2,5 kW Leistungsaufnahme gesamt
= 1,5 kW Overhead
Ziel: PUE 1,3 – 1,7

iX-TRACT

- Mit steigendem Stromverbrauch bewegt sich die IT-Branche nach allen Prognosen auch in den nächsten Jahren gegen den allgemeinen Trend.
- Da in vielen IT-Budgets die Energiekosten nicht berücksichtigt sind, haben IT-Abteilungsleiter oft keinen Überblick über den Stromverbrauch und dessen Verteilung. Den benötigt man aber, bevor man die Infrastruktur im Rechenzentrum optimieren kann.
- Als in vielen Umgebungen geeignete Energiesparmaßnahmen kristallisieren sich zwei heraus: die Server-Konsolidierung und energieeffiziente Kühllösungen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Wie grün sind Deutschlands Rechenzentren?

Rechenzentrum	Aufgaben	Größe	IT-Equipment	Kühlsystem
1&1, Karlsruhe	Webhosting, Dedicated Hosting, Virtual Dedicated Hosting, E-Mail-Services (einschließlich GMX und Web.de), interne Systeme	2000 m^2, 11 Rechnerräume	99 % Linux-Server, insgesamt 25 000; Dedicated Server werden speziell nach Anforderungen von 1&1 gebaut. 80+-Netzteile, auf unnötige Rechnerkomponenten wird verzichtet	8 Kompressions- und 3 Freikühler auf dem Dach; ab circa 10 °C Außentemperatur unterstützen Freikühler das System (einer der 8 Kompressionskühler als Redundanz); gesamte Kälteleistung circa 4,5 MW; kalte Luft wird durch Doppelboden direkt in die Racks geblasen
Claranet	Colocation, Dedicated Server, Managed LAMP-Server, Managed Application Hosting	2000 m^2 verteilt auf 3 Rechenzentren (Frankfurt am Main, 600 m^2, München 250 m^2, Berlin 150 m^2)	Cisco, Juniper, F5, Dell, HP	n+1-Klimatisierung von Stulz
Centron	Managed Server (Windows Server 2003/2008, Red Hat Enterprise & Debian Linux), Managed Cluster, Managed Storage, Managed Fail-Over & Load Balanced Solutions, Managed Streaming Solutions, Managed Data Center, Outsourcing & ASP, Software as a Service (SaaS), Housing, Colocation, E-Mail Hosting, Exchange Hosting, CRM Hosting, Webhosting, Managed Services (Microsoft Dynamics CRM 4.0, Sharepoint, Exchange 2003/2007, SQL 2005/2008, Monitoring Service, Total Performance Management, Backup und Disaster Recovery, Remote Hands Services, Installationsservice und -Support, Rapid Response	über 1000 m^2 verteilt auf 3 RZ-Standorte (1 × Frankfurt am Main, 2 × Nürnberg)	HP-Server, Supermicro-Server, Cisco only Networking, F5 Load Balancing, Rittal-Racksysteme	redundante 8,4 MVA Stromversorgung der Klimaanlagen, sensible Downflow-Klimakontrolleinheiten (redundant), zwei gespiegelte Klima-Kühlwassersysteme (redundant), Lufttemperatur 21 °C, relative Luftfeuchte 50 %
Host Europe	interne Systeme und Kunden-Systeme	bis zu 1700 m^2 nutzbare Rechenzentrumsfläche; 18 000 Server	Dell, Sun, Juniper, Cisco	Stulz-Klimageräte mit der Möglichkeit der freien Kühlung; durchgehend n+1-Redundanz
Hostway	Server Colocation, 24/7 Managed Services	3200 m^2	19-Zoll-Racks; redundantes Routing-Equipment; Juniper, Foundry, Cisco, zentrales Pillar-Date-Storage-System et cetera	Kaltwassersätze
Interoute	Managed Hosting, Virtual Hosting, Colocation, Datenbank-Management, Security, Netzwerkanbindung, Remote Hands Services	1100 m^2	HP, F5, EMC, Netapp, Cisco, Juniper, Checkpoint, Sun	24/7 Kontrolle von Raumtemperatur (22 °C, +/-2 °C) und Luftfeuchtigkeit (50 % rF, +/-10 %); die Klimatisierungsleistung ist größer als 1 kW pro qm; die Kühlung erfolgt durch den Doppelboden; alle Anlagen sind ebenfalls in n+1-Redundanz ausgelegt
IP-Exchange	Datentransport, RZ-Betrieb, IP-basierte Dienste	2 Rechenzentren in München und Nürnberg), zusammen 8000 Server auf 1800 m^2	Racks: Standard, Deluxe „Airflow“, High Cooling	Cold-Corridor-System, das auf dem Prinzip der kompletten Trennung von warmem und kaltem Luftstrom basiert
Strato	Webhosting, Serverdienstleistungen, Onlineshops, DSL-Anbieter	2 Rechenzentren (Karlsruhe, Berlin), insgesamt circa 4500 m^2	Shared Hosting Plattform: Sun T2000 und T5220-Server, NetApp FAS 6070 Massenspeicherplattform; Dedicated Hosting u. a. mit Quad-Core-AMD-Opteron-HE-Prozessoren, 750-GB-Festplatten im RAID1-Modus	mehrere redundante Kühlgeneratorenblöcke pro Serverraum; optimiertes Luftaustausch-management, u. a. mit abgeschlossenen kalten und warmen Gängen; freie Kühlung bei Temperaturen bis 8 °C

Ungefähr 50 000 bis 60 000 Rechenzentren gibt es insgesamt in Deutschland. Die meisten davon sind interne Data Center von Unternehmen, bei denen das Thema Energieeffizienz erst langsam an Präsenz gewinnt. Einige der Großen allerdings, wie zum Beispiel Webhoster, Onlineshop-Dienstleister oder Server Colocator, setzen sich schon seit Längerem mit Green IT in RZs auseinander.

Wartungsausfallzeiten, zum Beispiel bei einem Servertausch, und individuellen Patch-Services angefüllt.

Hier kann Virtualisierung helfen, die IT-Hardware effizienter einzusetzen. Dabei unterteilt man einen physischen Server in mehrere virtuelle, auf denen eigenständige Betriebssysteme unabhängig voneinander booten. Dadurch lässt sich die Serveranzahl signifikant reduzieren und die Auslastung bestehender Server auf bis zu 65 % steigern.

Zu beachten ist allerdings, dass man nicht jedes System konsolidieren kann. Deshalb ist eine gründliche Planung und Messung vorab unabdingbar. Insgesamt beträgt das Reduktionspotenzial der deutschen Unternehmens-IT durch Virtualisierung laut einer Studie von AT-Kearney schätzungsweise etwa 5 Mio. Tonnen CO_2 respektive 1 Mrd. Euro [4].

Mit einem gut durchdachten Kühlkonzept kann man den benötigten Strom effizient einsetzen. Dabei gibt es unterschiedliche Ansätze. Man unterscheidet zwischen Raum-, Reihen- und Rackküh-

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Virtualisierung	USV	Abwärmenutzung	Sonstiges
Im Shared Hosting wird eine speziell selbst optimierte Linux-Distribution eingesetzt, mit der die Daten von bis zu 10 000 Kunden auf einem Server verwaltet werden können. Aktuell sind in Karlsruhe rund 500 dieser Server im Einsatz. Seit Anfang 2006 werden virtuelle Server angeboten, auf denen sich ebenfalls mehrere Kunden befinden (bis zu 28 je nach Server-Typ und Ausstattung).	dynamische USV, 5 × 1100 kVA (davon 1 Block Redundanz); Verlustleistung etwa 7 %	derzeit keine, da im RZ Brauerstraße bautechnisch zu aufwendig	–
VMware ESX Cluster	n+1-redundante USV-Anlage von APC	–	–
Windows Virtual Server, Parallels Virtuozzo & VMware Virtualisierungs-Lösungen	4 × 2000 kVA Notstromgenerator, redundant gespiegeltes Notstromsystem (8,4 MVA), unterbrechungsfreie Stromversorgung (AC, DC) in n+1 bzw. 2n-Konfiguration, Batteriepufferung	–	hochsensible Brandfrühesterkennungs- und Meldesysteme, modernes Brandbekämpfungs-system (Foctec Nebeldüsen), VESDA-Rauchfrühwarnsystem und getrenntes Rauchmeldesystem, vibrationsfreie Umgebung; CCTV-System und 24-Stunden-365-Tage-Videoaufzeichnung; PAC-Sicherheitskarten-Zutrittskontrollsystem, Zugangs-Schleuse mit visueller Verifizierung, Personenvereinzelungsanlagen in Kombination mit biometrischen Zugangssystemen, Einbruchmeldeanlage
Partiell kommen Containervirtualisierung, Betriebssystemvirtualisierung und Paravirtualisierung zum Einsatz.	APC-Anlagen mit externen Batterieblöcken, n+1-Redundanz; dieselbetriebene Notstromgeneratoren mit bis zu 6 MVA	Nutzung der Abwärme durch Wärmepumpen für die Heizung der gesamten Büroetage	–
Virtuozzo, VMware, Xen	RZ-weite Batteriepufferung; 4 dieselgetriebene Notstromgeneratoren	Über Wärmerückgewinnung werden eigene sowie die umliegenden Gewerbeflächen geheizt.	–
VMware, XEN, Hyper-V	dieselgetriebene Notstromgeneratoren (3 × 400 kW), n+1 redundant; Dieselkraftstoff-Bevorratung von 12 000 Litern (entspricht einer autarken Versorgung von mindestens 72 Stunden)	–	–
✓ (mit Green CIO-Award ausgezeichnet)	mehrere Transformatorstationen mit redundanter Zuführung der Versorger; nachgeschaltet diverse n+1-USV-Anlagen mit zusätzlicher Notstromspeisung aus Dieselaggregaten; Infrastruktur gemäß Tier-III/Tier-IV-Kategorie D; Geräte mit 2 Netzteilen (ohne doppelten Stromverbrauch)	–	Stromzähler, die auf jedem Rack installiert werden können; Einsatz regenerativer Energiequellen
Shared Hosting: dynamische Lastkonfiguration der Plattform (freie Ressourcen können sowohl der Web-, als auch der Mail- und der Datenbankfarm zugeordnet werden) sowie reziproke Virtualisierung; Dedicated Hosting: virtuelle Server für Privatkunden, maximal 10 Kunden pro System, Virtualisierungssoftware Virtuozzo von SWsoft	AEG SVS Protect 4	–	detailliertes und kontinuierliches Monitoring des Energieverbrauchs durch Sensoren in allen Bereichen der Rechen-zentren; Betrieb der Rechenzentren mit Regenerativstrom aus Laufwasserkraft (NaturEnergie AG)

lung. Wenn eine Modernisierung der Infrastruktur ansteht, haben sich einerseits Rackkühlungen für einzelne „Hitzeschleudern“ und andererseits sogenannte Kaltgang/Warmgang-Anordnungen für viele Stromfresser besonders bewährt. Eine Optimierung bringt eine Kaltgangbeziehungsweise eine Warmgangeinschottung, bei der der Gang komplett geschlossen ist. So vermischt sich die kalte Luft nicht mit der warmen.

Einen ähnlichen Effekt haben moderne Doppelboden-Umluftsysteme, bei denen Ventilatoren im Boden integriert sind, die die Kaltluft gezielt in einzelne Racks blasen. Auch eine saubere Abdichtung, etwa mit Bürstensystemen, gewährleistet eine bessere Energienutzung. Außerdem empfiehlt sich der Einsatz von Aggregaten mit höherem Wirkungsgrad und eine Erhöhung der Rechenzentrumstemperatur, denn Rechenzentren können durchaus bei Temperaturen von bis zu 26 °C laufen – manche Experten sprechen heute sogar von 30 °C. Allerdings haben Forschungen von IBM in Zusammenarbeit

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Green-IT-Projekte der Big Five

Alle Anbieter von Rechenzentrumskomponenten springen derzeit auf den „Green-IT-Zug“ auf – zum einen aufgrund des tatsächlich vorhandenen Handlungsbedarfs, aber auch wegen des nicht von der Hand zu weisenden Verkaufsarguments der massiven Kosteneinsparung. Dabei gehen die „Big Five“, die als einzige Anbieter die komplette Rechenzentrumsausstattung inklusive Netzwerk, Server und Storage im Programm haben, als gute Vorbilder voran und haben ihre bis zu über hundert Rechenzentren auf eine einstellige Anzahl reduziert.

IBM – Projekt „Emissionsfreies Rechenzentrum“

Mit umfassenden Konsolidierungsmaßnahmen hat beispielsweise IBM im Rahmen des Projekts „Big Green“ bis zu 80 % der eigenen RZ-Kosten gesenkt und spart dadurch den Strombedarf einer Kleinstadt.

Zukunftsweisendes Projekt von IBM ist allerdings das „Emissionsfreie Rechenzentrum“, das Forscher des Züricher Forschungszentrums auf der Cebit 2008 erstmals vorgestellt haben. Im Mittelpunkt steht dabei die Energiewiederverwendung. Die Entwickler setzen auf ein neuartiges Wasserkühlsystem, das über Mikrotechnik-Kühler direkt auf den Chip geht. Die Herausforderung: Um Abwärme effizient nutzen zu können, muss die Schwellentemperatur bei ungefähr 50 °C liegen. Die erreichen sie durch 45 °C warmes Vorlaufwasser.

Noch ist das Projekt des emissionsfreien Rechenzentrums nicht in Serie gegangen. Das IBM-Labor allerdings nutzt es selbst erfolgreich. Ein weiteres aktuelles Forschungsobjekt ist die Wasserkühlung von 3-D-Chips, womit sich ganz neue Perspektiven für die Entwicklung hochperformanter Chips ergeben.

Hewlett-Packard – Energie-Management-System

Eine der jüngsten Entwicklungen aus den HP-Labs ist Dynamic Smart Cooling (DSC), eine Energie-Management-Lösung für deutliche Einsparungen bei der Kühlung von Server-Räumen und Rechenzentren. Sie basiert auf einer Software in einem Kontrollknoten, der die Leistung der Klimaanlage kontinuierlich an den tatsächlichen Bedarf anpasst. Hierzu erfasst das System mit einem Netz von Sensoren an den Racks die aktuellen Lufttemperaturen in Echtzeit. Dynamic Smart Cooling kann dadurch dort kühlen, wo es tatsächlich notwendig ist. So sollen sich der Stromverbrauch und die Kosten für die Kühlung um 45 % senken lassen.

Sun – Pionier auch für „grüne“ Prozessoren

Als Sun 2005 den Ultrasparc T1 Prozessor unter dem Codenamen Niagara vorstellte, war von Green IT noch nicht die Rede. Geschweige denn, dass jemand die Bedeutung, die grüne IT-Strategien einnehmen würden, absehen konnte. Der Gedanke hinter dem bis heute einzigartigen Prozessordesign: Je mehr Auslastung, desto besser die Effizienz. Also baut Sun Prozessoren, die viele Arbeitsschritte gleichzeitig ausführen können und auf bestimmte Anwendungen spezialisiert sind. Beim Ultrasparc T1, der das Multi Threading unterstützt, können acht Prozessorkerne mit jeweils vier Threads 32 Aufgaben quasi gleichzeitig ausführen.

Den aktuellen Ultrasparc T2 (Niagara 2) bezeichnet Sun inzwischen als „ersten Server auf einem Chip“. Er besitzt neben nunmehr acht Kernen mit je eigenen Floating Point Units und acht Threads pro Kern zusätzliche Krypto- und 10-GBit-Ethernet-Engines. Mit den 64 quasi-parallelen Prozessen erreicht Sun mehr als durch eine Erhöhung der Taktrate oder eine Cache-Vergrößerung. Der Sun-Prozessor ist mit maximal 1,4 GHz getaktet.

Fujitsu Siemens Computers – Dreistufenkonzept für alle

Fujitsu Siemens Computers hat für die Senkung der Energiekosten in Rechenzentren ein Dreistufenkonzept entwickelt, das allen seinen energieeffizienten Produkten zugrunde liegt. Es lässt sich zur Orientierung bei der Energieeffizienzoptimierung des eigenen Rechenzentrums nutzen:

Erstens lässt sich der Stromverbrauch reduzieren, indem man durch verbesserte Chips und Herstellungsprozesse den Energiebedarf von Prozessoren und I/O-Chips senkt, die Rechenleistung pro Watt Leistungsaufnahme sowie den Wirkungsgrad von Server-Stromversorgungen erhöht.

Zweitens kann man die Rechenzentrumsinfrastruktur optimieren durch die Verbesserung der Kühlkonzepte und der Energieinfrastruktur sowie die Energiewiedergewinnung im Rechenzentrum.

Drittens kann man die Auslastung vorhandener Ressourcen erhöhen durch Konsolidierung – es werden weniger und leistungsfähigere Systeme eingesetzt –, durch die verbesserte Auslastung von IT-Systemen per Virtualisierung, durch die flexible Steuerung des Energieverbrauchs mithilfe dynamischer IT-Lösungen und durch die Bestimmung des richtigen Gleichgewichts zwischen Energieaufwand und optimaler Server-Performance.

Vor allem die Verwendung virtueller Maschinen soll bestehende Rechnerkapazitäten optimal nutzen. Auf diese Weise lässt sich ein Wirkungsgrad von fast 100 % der eingesetzten Energie erreichen. Zudem setzt FSC auf Systeme für das automatische Abschalten der nicht verwendeten Hardware – in Kombination mit einer Reduzierung des CPU-Taktes und der I/O-Bandbreite, der Vermeidung von Spitzen im Lastprofil und der Reduzierung der Kühlungs- und Energieinfrastruktur im Rechenzentrum.

Dell – ganzheitlicher Energieeffizienz-Service

Dell versteckt sich hinter seiner Energy-Smart-Lösung: den Poweredge-Servern, kombiniert mit der Kühltechnik Liebert XD und dem Kühlsystem Liebert High Precision Air Conditioning von Emerson Network Power. Die Kombination soll den Stromverbrauch gegenüber Poweredge-Vorgängermodellen um bis zu 42 % reduzieren, bei einer gleichzeitigen Steigerung der Systemperformance um bis zu 80 %.

Darüber hinaus hat Dell neue Energy-Smart-Services entwickelt, mit denen Unternehmen in der Lage sind, Kühl-Ineffizienzen aufzuspüren, Rechenzentrums-Infrastrukturen und Systemkapazitäten zu evaluieren, die Rechenkapazitäten zu optimieren und den Energieverbrauch zu reduzieren. Außerdem stellt Dell für Vorher-Nachher-Schätzungen Energiekalkulatoren zur Verfügung, sogenannte Datacenter Capacity Planner sowie Whitepaper und erstellt im Rahmen von Datacenter Environmental Assessments vor Ort beim Kunden Bestandsaufnahmen zu Energieverbrauch und vorhandener Infrastruktur.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

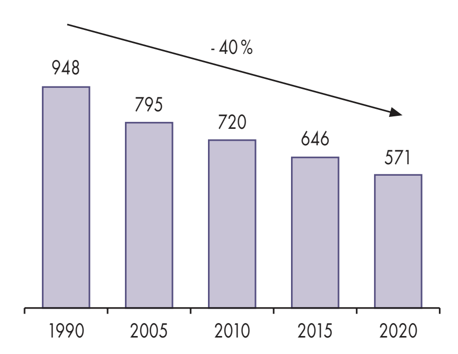
mit der DEKA und dem TÜV ergeben, dass es ein Optimum des Verhältnisses zwischen Raum- und Servertemperatur gibt, bei der ein Server selbst seine Betriebstemperatur nachregeln kann.

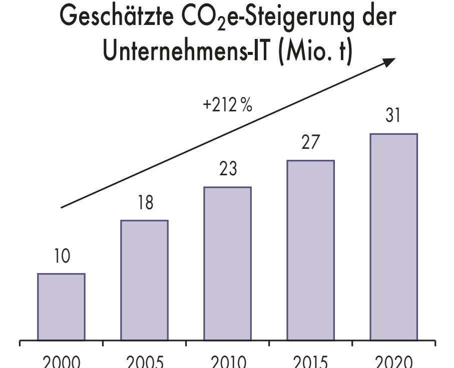
Gar nicht neu – Wasser und Brennstoffzellen

Bauliche Veränderungen sind oftmals nötig, wenn man zudem die Außenluft zur Kühlung einsetzen will oder die Zweitverwertung der Abwärme für die Gebäudeheizung anstrebt. Noch eins ist wichtig: Ein Generalrezept für ein grünes Rechenzentrum gibt es nicht. Es spielen immer die zugrunde liegenden Bedingungen des RZ-Umfelds eine Rolle. So kann man dort mehr Energie sparen, wo sich das Data Center in einem Keller befindet, die Außentemperaturen aufgrund des Klimas niedriger sind oder, wie bei BMW, kaltes Wasser direkt aus einem Brunnen für die Kühlung zur Verfügung steht.

Letztlich spielt in Zukunft auch die Frage eine entscheidende Rolle, ob man von der derzeit vorherrschenden Luftkühlung wieder auf Wasserkühlung umstellen sollte, da Wasser Wärme 4000-mal besser abführen kann. In diesem Punkt allerdings scheiden sich bei den Herstellern noch die Geister. Dell zum Beispiel bietet Systeme an, die völlig ohne Klimaanlage auskommen und nur auf Lüftung oder auf einfach konstruierte, aber zugleich hocheffiziente Verdunstung setzen.

Für die unterbrechungsfreie Stromversorgung (USV) sehen einige ein großes Zukunftspotenzial in der Brennstoffzelle. Lange Autonomiezeiten, Skalierbarkeit, keine Schadstoffe und geringer Wartungsaufwand sind ihre Vorteile. Außerdem sind die Überbrückungszeiträume flexibel planbar. Hinzu kommt, dass Brennstoffzellen umweltfreundlich sind, da als Nebenprodukte lediglich Wärme und Wasser entstehen. So sorgt die Brennstoffzelle als USV für eine autarke, umweltfreundliche und wirtschaftliche Energieversorgung. Allerdings ist die Technik neu und trifft auf Vorbehalte am Markt. Es geht aber weniger darum, bestehende USV-Systeme zu ersetzen, als die Brennstoffzelle bei einer Neuplanung überhaupt ins Kalkül zu ziehen. Zudem gibt es mittlerweile sehr effiziente Kombinationen aus Brennstoffzelle und regenerativen Energien, wie Photovoltaik oder Windkraft.





Gegen den Trend: Ohne Gegenmaßnahmen steigt die durch die IT verursachte CO_2e-Produktion in Deutschland von 2000 bis 2020 um das Dreifache. Gründe dafür sind unter anderem der höhere Durchdringungsgrad der IT, zunehmende Internetnutzung und die Verbreitung rechenintensiver Architekturen (Abb. 1).

Insgesamt haben diese Maßnahmen ein Stromsparpotenzial von 15 bis 20 % für deutsche Rechenzentren. Dies entspricht einem verringerten CO_2-Ausstoß um 1 Mio. Tonnen oder 0,2 Mrd. Euro pro Jahr an eingesparten Stromkosten [4].

Fazit

Auch wenn Konsolidierung und Kühlung die zwei Hauptthemen in puncto energieeffiziente Rechenzentren sind, haben die einzelnen Hersteller von Rechenzentrumskomponenten unterschiedliche Strategien der Energiereduktion entwickelt. Es ist schier unmöglich, auch nur im Ansatz alle Produkttrends der einzelnen Hersteller im Bereich „Grünes Rechenzentrum“ aufzuzeigen.

Wichtig ist es aber für jeden Rechenzentrumsbetreiber, zu verstehen, dass in Zukunft die Energiekosten die Anschaffungskosten bei Weitem überschreiten werden. Außerdem wird man um die Einsicht nicht herumkommen, dass das Thema „Grünes Rechenzentrum“ ein sehr komplexes ist und es nicht genügt, hier und da einen „Stromfresser“ zu beseitigen. Wie ausführlich gezeigt, muss es in erster Linie darum gehen, die Systeme optimal auszulasten, auf modulare Lösungen zu setzen und ein gutes Verhältnis zwischen Energieverbrauch und Leistung zu erreichen. Letztlich kommt es auf eine detaillierte individuelle Planung und Umsetzung an. Denn jedes Rechenzentrum weist andere Rahmenbedingungen in puncto Räumlichkeiten, Leistungsbedarf und machbaren Energieeinsparungen auf. (sun)

JANA BEHR

ist freie IT-Redakteurin.

Literatur

[1] Borderstep-Institut; Zukunftsmarkt energieeffiziente Rechenzentren; Studie im Auftrag des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit (BMU); Berlin 2007

[2] Forschungsstelle für Energiewissenschaft/Fraunhofer-Institut für System- und Innovationsforschung/TU Dresden (Hrsg.); Technische und rechtliche Anwendungsmöglichkeiten einer verpflichtenden Kennzeichnung des Leerlaufverbrauchs strombetriebener Haushalts- und Bürogeräte; Kurzfassung des Abschlussberichts an das Bundesministerium für Wirtschaft und Arbeit; Karlsruhe/München/Dresden 2005

[3] Daniel Spreng, Andrea Scheller, Brigitte Schmieder, Nicola Taormina; Das Energieverbrauchsfenster, das kein Fenster ist; CEPE Working Paper Nr. 15 (Schweizer Center for Energy Policy and Economics); Juni 2002

[4] Studie „Von Green IT zu Green Business“ von ATKearney, 2008

[5] Bitkom; Energieeffizienz im Rechenzentrum; Ein Leitfaden zur Planung, zur Modernisierung und zum Betrieb von Rechenzentren; 2008; www.bitkom.org/files/documents/Leitfaden_Energieeffizienz_in_RZ_final_31072008.pdf

[6] Präsentation „Green RZ“ – Was steckt dahinter?; Vossel Solution GmbH 2008

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Document Driven Development mit dem Fit-Framework

Rettet die Dokumente!

Oliver Böhm

Zu den ungeliebtesten Aufgaben in der Softwareentwicklung gehört die Dokumentation – obwohl jeder weiß, wie wichtig sie ist. Wer es schafft, Dokumente während des Entwicklungsprozesses zu aktualisieren und so am Leben zu erhalten, kennt nicht nur stets den aktuellen Projektstatus, sondern kann sich gleichzeitig durch Integrationstests das Leben erleichtern.

Wer kennt das nicht? Man kommt als Neuer in ein bestehendes Projekt und muss sich erst einmal einarbeiten. Dummerweise sind alle ziemlich beschäftigt, sodass man allein auf Pflichtenheft, Fachkonzept, Architektur-Dokumente und Entwickler-Handbücher angewiesen ist. Glücklicherweise sind diese vorhanden, führen aber oft in die Irre. Es stellt sich heraus, dass große Teile der Dokumentation veraltet sind und dem aktuellen Stand von zwei Versionen hinterherhinken.

Als einzig verlässliche Quelle bleibt der Sourcecode selbst. Noch immer ist Dokumentation unter Entwicklern (und nicht nur dort) unbeliebt, obgleich das V-Modell und andere Vorgehensmodelle so viel Wert drauf legen. Um das zu verstehen, sollen die folgenden Ausführungen ein traditionelles Dokument auf seinem Weg von der Wiege bis zur Bahre begleiten.

Das Leiden des Dokuments X

Dabei soll es sich vor allem darum drehen, wie sich mit einem kleinen Trick Dokumente gegen Alterung schützen lassen. Mithilfe von Fit (Framework for Integrated Test, siehe „Onlinequellen“) und eines Document-Driven-Development-Ansatzes (DDD) kann man erreichen, dass der Projektfortschritt in der Softwareentwicklung sichtbar wird und Integrationstests ihren Schrecken verlieren.

Anhand eines Fachkonzepts einer E-Banking-Anwendung lassen sich einige typische Probleme identifizieren, die so oder ähnlich in vielen Projekte auftauchen. Entwickler erstellen Fachkonzepte oft widerwillig und unter Zeitdruck. Viele Fragen lässt schon das Pflichtenheft offen, die ein Projektteam in der Kürze der Zeit und trotz der vielen ungeliebten Abstimmungs-Meetings nicht alle klären kann. Und um nichts Falsches ins Fachkonzept zu schreiben, sind viele Passagen wie der folgende Ausschnitt zur Login-Maske ziemlich unverbindlich gehalten – schließlich soll das Dokument ja irgendwann mal fertig werden:

„… Die Login-Maske bietet die Möglichkeit, sich mit einer Benutzerkennung und der PIN anzumelden. Wird eines der beiden Felder nicht ausgefüllt, wird dem Benutzer eine entsprechende Fehlermeldung angezeigt …“

Ist das Fachkonzept erstellt und abgenommen, ist damit oft auch sein Tod vorprogrammiert. Mit der Abnahme gibt es niemanden mehr, der für das Dokument verantwortlich zeichnet. Jeder ist froh, dass es endlich fertig ist,

iX-TRACT

- Fachkonzepte entstehen häufig unter Zeitdruck und gehören zudem zu den ungeliebten Aufgaben von Entwicklern. Testfälle für die Integrationstests werden häufig aus ungenauen und lückenhaften Fachkonzepten abgeleitet.
- Ein Vorgehen, das dem Document Driven Development entspricht, und der Einsatz des Fit-Framework lassen Fehler und unzureichende Spezifizierung während des Entwicklungsprozesses offenkundig werden.
- Durch den Einsatz von Tabellen kann der Entwickler solche Lücken schließen und zudem eine solide Basis für den Entwurf von Integrationstests schaffen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

und kein Entwickler wird es freiwillig anpassen oder korrigieren, sondern neue Erkenntnisse oder Änderungen direkt in Code gießen. Mitarbeiter, die später zum Projekt dazustoßen, haben Pech – sie finden ein veraltetes Dokument vor, in dem Dinge fehlen oder nicht mehr richtig sind.

Kurzum, der Lebenszyklus (oder besser „Leidensweg“) eines Dokuments lässt sich so zusammenfassen:
– schwere Geburt (oft mit vielen Wehen verbunden)
– schwieriges Wachstum (ungeliebtes Kind, viel Arbeit, wenig Freude)
– früher Tod (keine Eltern, keine Pflege)
Mit fortlaufender Projektdauer nimmt die Übereinstimmung des Dokuments mit den Anforderungen und damit seine Qualität immer mehr ab.

Ein weiteres Problem mit dem Fachkonzept zeigt sich bei den Integrationstests, für die bei größeren Projekten oft eine eigene Testabteilung zuständig ist. Testfälle werden meist in Form von Excel-Tabellen aus dem Fachkonzept oder Pflichtenheft abgeleitet.

Leider gibt das Fachkonzept nicht alle für das Testen benötigten Daten her, sodass oft Rücksprachen mit der Fachabteilung (oder dem Auftraggeber) nötig sind. Das Ergebnis einer solchen Zusammenarbeit ist in Tabelle 1 an der Fehlermeldung in der Spalte „Erwartetes Ergebnis“ zu sehen, das so konkret weder im Fachkonzept noch im Pflichtenheft stand. Fehler im Fachkonzept offenbaren sich ebenfalls meist erst beim Ableiten der Testfälle.

Tabelle 1: Auszug aus einem Testdokument

lfd. Nr.	Voraussetzung	Testeingabe	erwartetes Ergebnis	Ergebnis	Art der Abweichung
...	...	...	...		
25	Benutzer steht auf Anmeldemaske	leere Benutzerkennung	Fehlermeldung: Im Feld „Benutzerkennung“ ist für die Bearbeitung eine Eingabe erforderlich.		
26		gültige Benutzerkennung, leere PIN	Fehlermeldung: Im Feld „PIN“ ist für die Bearbeitung eine Eingabe erforderlich.		
...	...	...	...		

Tabelle 2: Fehlermeldungen bei fehlender Eingabe

Benutzerkennung	PIN	Fehlermeldung
47118015	12345	keine Fehlermeldung
	12345	Im Feld „Benutzerkennung“ ist für die Bearbeitung eine Eingabe erforderlich.
47118015		Im Feld „PIN“ ist für die Bearbeitung eine Eingabe erforderlich.

Tabelle 3: Angepasste Kopfzeilen für Fit

giropay.blackbox.fit.fixture.LoginFixture		
Benutzerkennung	**PIN**	**Fehlermeldung()**
47118015	12345	keine Fehlermeldung
	12345	Im Feld „Benutzerkennung“ ist für die Bearbeitung eine Eingabe erforderlich.
47118015		Im Feld „PIN“ ist für die Bearbeitung eine Eingabe erforderlich.
		Im Feld „Benutzerkennung“ ist für die Bearbeitung eine Eingabe erforderlich. Im Feld „PIN“ ist für die Bearbeitung eine Eingabe erforderlich.

Tabelle 4: Ergebnis nach dem Fit-Lauf

giropay.blackbox.fit.fixture.LoginFixture		
Benutzerkennung	**PIN**	**Fehlermeldung()**
47118015	12345	keine Fehlermeldung
	12345	Im Feld „Benutzerkennung“ ist für die Bearbeitung eine Eingabe erforderlich.
47118015		Im Feld „PIN“ ist für die Bearbeitung eine Eingabe erforderlich.
		Im Feld „Benutzerkennung“ ist für die Bearbeitung eine Eingabe erforderlich. Im Feld „PIN“ ist für die Bearbeitung eine Eingabe erforderlich. *expected* Im Feld „Benutzerkennung“ ist für die Bearbeitung eine Eingabe erforderlich. *actual*

Rückgriff auf Altbekanntes

Einen Ausweg aus dem Dilemma mit ungepflegten Dokumenten und fehlendem Test-Input bietet das Fit-Framework von Ward Cunningham, der schon mit dem Ur-Wiki eine einfache, aber mächtige Anwendung geschaffen hat. Die Grundidee hinter Fit ist, dass Tester keine neue Testsprache brauchen, sondern dass eine Unterstützung auf dem aufbauen soll, was sowohl Tester als auch die Experten aus der Fachabteilung beherrschen – den Umgang mit (Excel-)Tabellen.

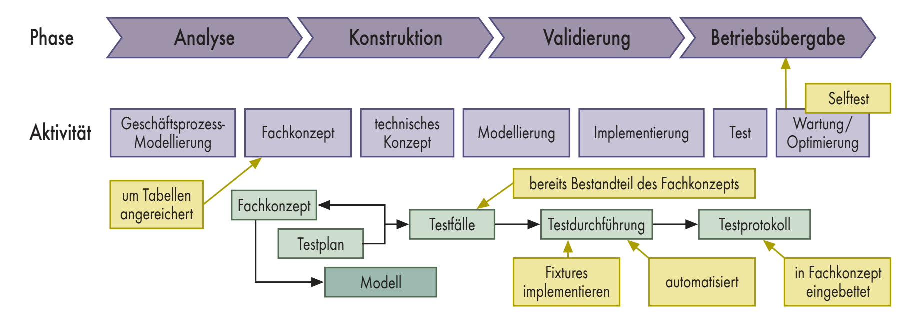
Für den Einsatz von Fit wird das Fachkonzept um Tabellen angereichert, die das Team später für eine Automatisierung des Integrationstests heranziehen kann. Das Eingangsbeispiel wird dabei um Tabelle 2 ergänzt:

Für den Autor des Fachkonzepts bedeutet das zunächst Mehrarbeit, die sich erst viel später beim Testen bezahlt macht. Er muss nicht nur die Tabellen erstellen, sondern es sind zusätzliche Absprachen mit der Fachabteilung oder dem Auftraggeber nötig – hier beispielsweise für die gewünschte Fehlermeldung. Allerdings darf man nicht vergessen, dass das Fachkonzept die Grundlage für die anschließende Entwicklung ist und diese Angaben spätestens hier benötigt werden.

Tabellen werten das Dokument auf und machen es konkreter und verständlicher (und damit die Entwicklung geradliniger). Manche Unklarheit lässt sich so im Vorfeld ausräumen, was unter Umständen teure Fehlentwicklungen



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Das Fit-Framework integriert sich nahtlos in den Entwicklungsprozess (Abb. 1).

vermeidet. Beispielsweise lässt sich die Tabelle leicht um eine Fehlermeldung für den Fall ergänzen, dass überhaupt keine Eingabe erfolgt (siehe Ende Tabelle 3). Unter anderem ergeben sich offene Fragen, wenn man noch in Kontakt mit der Fachabteilung oder dem Auftraggeber ist. Der Entwickler findet sich zudem viel schneller zurecht, da alles Wichtige in Tabellen zusammengefasst ist, und der Tester erhält konkrete Vorgaben für Testfälle. Darüber hinaus kann er die Tabellen mithilfe von Fit als Eingabe für automatisierte Tests nutzen.

Hierfür muss er die Tabellen noch ein wenig anpassen. Entscheidend ist dabei der Kopf der Tabelle (siehe Tabelle 3).

In der ersten Zeile (hier: *giropay.blackbox.fit.fixture.LoginFixture*) muss im Beispiel eine Java-Klasse stehen, die das Framework aufrufen kann und die im Fit-Sprachgebrauch als „Fixture“ bezeichnet wird. Diese Klasse muss die Bedeutung der einzelnen Spalten kennen, wobei sie durch das Framework unterstützt wird. Dazu wurde die zweite Zeile etwas angepasst und in Eingabe-Spalten und Ausgabe-Spalten aufgeteilt: Erstere haben das Aussehen von Java-Attributen (hier: Benutzerkennung, PIN), Ausgabe-Spalten sehen durch das angehängte Klammern-Paar aus wie eine Methode (hier: Fehlermeldung()). Dies entspricht der Notation, die Fit im Fixture erwartet (siehe Listing 1).

Das Fit-Framework belegt die beiden Attribute *Benutzerkennung* und *PIN* vor, bevor es die Methode *Fehlermeldung()* aufruft. Für einen automatisierten Test muss der Entwickler lediglich *LoginFixture* von der Oberklasse *ColumnFixture* ableiten und die *Fehlermeldung()* implementieren.

Fit liefert einen FileRunner mit, der zwar nur HTML-Dateien lesen kann, aber sowohl Word als auch Excel können Dokumente nach HTML exportieren. Das Ergebnis gibt der FileRunner in Form einer kommentierten Kopie des Dokuments aus. Ob ein Testfall erfolgreich war, protokolliert Fit über die Tabellen innerhalb dieses Dokuments (vgl. Tabelle 4):
– War der Test erfolgreich, hinterlegt Fit den Tabelleneintrag grün.
– Weicht das Ergebnis von der Vorgabe ab, wird der Unterschied angezeigt und der Eintrag erscheint auf rotem Hintergrund.
– Das Auftreten einer Exception zeigt das Framework ebenfalls an und markiert sie gelb.

Aus Tabelle 4 ist relativ schnell die fehlende zweite Fehlermeldung ersichtlich, deren Fehlen jetzt schon während der Entwicklung auffällt und nicht erst später während des Integrationstests offensichtlich wird.

Das Dokument lebt

Bei der anfangs erwähnten E-Banking-Software stellte sich im Verlauf der Entwicklung heraus, dass die Schnittstelle, über die das Backend angesprochen wird, allergisch auf Sonderzeichen reagiert. Eine Rücksprache mit den Fachleuten ergab, dass die Prüfung von gültigen Zeichen bereits im Frontend erfolgen muss. Weder im Pflichtenheft noch im Fachkonzept war das spezifiziert.

Meist ist der notwendige Änderungsaufwand an bestehenden Dokumenten zu hoch, sodass in vielen Projekten ein Entwickler die fehlenden Prüfungen direkt implementiert, ohne sie zu dokumentieren. Damit setzt ein schleichender Alterungsprozess des Dokuments ein.

Mit dem Fit-Ansatz ist es relativ einfach, das Fachkonzept anzupassen: Es gibt ja bereits eine Tabelle mit erlaubten und unerlaubten Eingabe-Kombinationen, die sich schnell erweitern lässt (siehe Tabelle 5).

Da bereits eine Implementierung von *LoginFixture* vorliegt, muss man nur einen weiteren Testlauf starten und erhält unmittelbares Feedback, ob die Software das Gewünschte leistet.

Auf diese Art und Weise führen neue Erkenntnisse zu neuen Testfällen und man erhält ein lebendes Dokument. Durch den automatischen Ablauf der Tests erkennt der Entwickler zudem schnell, ob das Dokument mit der Software übereinstimmt. Manchmal stellt sich auch heraus, dass nicht die Software, sondern das Fachkonzept falsch ist. Auf jeden Fall erfolgt eine unmittelbare Rückmeldung darüber, inwieweit Dokumentation und Implementierung kongruent sind.

Als größte Hürde beim Einsatz von Fit erwies sich das mühsame Erstellen der Tabellen mit Word. Immerhin hat sich die Mühe gelohnt. Sowohl der Auftraggeber als auch die Geschäftsleitung haben dem Team für das Fachkonzept Lob gezollt – offensichtlich hob es sich allein durch seine Tabellen

Tabelle 5: um Eingabe von Sonderzeichen erweitert

giropay.blackbox.fit.fixture.LoginFixture		
Benutzerkennung	PIN	Fehlermeldung()
47118015	12345	keine Fehlermeldung
	12345	Im Feld „Benutzerkennung“ ist für die Bearbeitung eine Eingabe erforderlich.
47118015		Im Feld „PIN“ ist für die Bearbeitung eine Eingabe erforderlich.
		Im Feld „Benutzerkennung“ ist für die Bearbeitung eine Eingabe erforderlich. Im Feld „PIN“ ist für die Bearbeitung eine Eingabe erforderlich.
%%%	12345	Die Eingabe im Feld „Benutzerkennung“ ist ungültig.

Listing 1: Klasse *LoginFixture*

```
public class LoginFixture extends ColumnFixture {

    public String Benutzerkennung;
    public String PIN;

    public String Fehlermeldung() {
        String errorMsg = login(Benutzerkennung, PIN);
        if (StringUtils.isEmpty(errorMsg)) {
            return "keine Fehlermeldung";
        } else {
            return errorMsg;
        }
    }
    ...
}
```

Mit diesem Fixture kann das Fit-Framework Tabelle 3 überprüfen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

positiv vom Rest des Projekts ab. Die Befürchtung, dass der Tabellenkopf durch die Angabe des Testtreibers (Fixture) oder durch die notwendige Java-Namenskonvention negativ auffiel, erwies sich als unbegründet.

Erfahrungen aus dem Projektalltag

Etwas heikel war die Erweiterung des Fachkonzepts. Schließlich handelt es sich dabei um ein offiziell abgenommenes Dokument, das als Basis für die abgegebene Schätzung dient. Daher hat das Team Änderungen in einem eigenen Anhang zusammengefasst. Zusätzlicher Aufwand (etwa die Prüfung der Eingabe) wurde dadurch deutlicher sichtbar und konnte mit dem Auftraggeber diskutiert werden.

Parallel zur Erstellung des Fachkonzepts implementierte das Projektteam leere Testklassen. Damit ließ sich mit der Abnahme des Fachkonzepts bereits ein erster Integrationstest starten. Zwar schlugen noch alle Tests fehl (genauer gesagt lieferte das Fit-Framework Exceptions, weil Attribute und Methoden noch fehlten), aber es lag eine Ausgangsbasis für die zweiwöchigen Arbeitsplanungen vor. Die Tests, die noch nicht liefen, wurden für den nächsten Zyklus geplant und aufgeteilt. Zwei Vorteile ergaben sich dadurch:

– Der Projektfortschritt wurde sichtbar und
– das Team erhielt durch den TDD-Ansatz eine testbare Architektur und konnte Refactorings gelassener angehen.

Unsicherheit herrschte bei der Frage, ob Fit die JUnit-Tests überflüssig machen würde, beziehungsweise wie sich die beiden Test-Frameworks voneinander abgrenzen. Der Name verrät es schon: Fit ist für den Integrationstest vorgesehen. Deswegen dürfen Fit-Tests schon mal länger dauern (und tun es auch), da sie nicht so häufig aufgerufen werden. JUnit-Tests hingegen sind Entwickler-Tests, die die Funktion einer einzelnen Klasse testen. Ihr Aufruf erfolgt im Idealfall bei jeder Änderung der Klasse, daher müssen sie schnell sein.

Leider hat das Projektteam es aus Zeitmangel nicht geschafft, alle Fit-Tests auf grün zu bekommen, da das Schreiben der Test-Treiber auch Zeit kostet – hier musste man abwägen, ob sich für einige Tabellen der Aufwand lohnt. Es blieben aber genügend „grüne“ Tabellen übrig, die die Integration erleichterten und die manuelle Tests zwar nicht überflüssig machten, aber die Arbeit dafür erheblich reduzierten.

Ein willkommener Zusatznutzen ergab sich für den Betrieb, da die Auslieferung der Fit-Tests inzwischen zusammen mit einer kleinen Weboberfläche erfolgt. Dadurch kann der Administrator die Anwendung und die Konfiguration während des Betriebs jederzeit überprüfen.

Fazit

Der Einsatz des Test-Framework hat sich in mehreren Projekten bewährt und ist inzwischen fester Bestandteil des Vorgehensmodells (s. Abb. 1). Angefangen von der Analyse mit der Erstellung des Fachkonzepts erstreckt sich das Fit-Einsatzgebiet bis hin zur Betriebsübergabe als Diagnose-Werkzeug.

Etwas nachteilig wirkt sich der zusätzliche Aufwand bei der Erstellung der Dokumente aus – kein Entwickler oder Architekt dokumentiert gern. Aber dieser Mehraufwand macht sich schnell bezahlt, und die Akzeptanz von Fit innerhalb des Projektteams war sehr hoch.

Dabei ist Fit nicht auf Java beschränkt. Auf der Fit-Homepage finden sich Links zu anderen Sprachen, aber auch Tools, die das Framework erweitern oder darauf aufbauen. Sein Einsatz bietet viele Vorteile, von denen dieser Artikel nur einen Teil aufführen konnte:

– Dokumente werden verständlicher.
– Missverständnisse treten deutlich früher zutage.
– Die Dokumentation ist aktueller (Dokumente müssen gepflegt werden, sonst schlagen Tests fehl).
– Hierarchische Dokumente sind möglich.
– Die Dokumente sind auch für Akzeptanz- und GUI-Tests geeignet.
– Mit dem Framework entwickelte Projekte erlauben automatisierte, kontinuierliche Integrationstests und die Einbindung in den Build-Prozess von Ant oder Maven. Mit Fit sind Dokumente nicht mehr Teil des Problems, sondern Teil der Lösung. (ka)

Onlinequellen

DDD	www.agentes.de/ddd/
Fit	fit.c2.com
Fit-Einführung	oli.blogger.de/20080413/
JUnit	www.junit.org
Westphal	www.frankwestphal.de/TestgetriebeneEntwicklungmitJUnitundFIT.html

OLIVER BÖHM

arbeitet als J2EE-Entwickler und -Coach bei der Agentes AG und ist unter anderem Autor des Buches „Aspekt-Orientierte Programmierung mit AspectJ 5“.





Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Individuelle Optimierung von Echtzeit-Anwendungen

Ganzheitliches Tuning

Amjad Mohsen

In Anwendungsbereichen wie der digitalen Signalverarbeitung ersetzen zunehmend High-Level-Synthese-Werkzeuge traditionelle Entwurfsmethoden. Doch macht das individuelle Anpassungen wirklich überflüssig?

Etwa zwei Drittel aller Elektronik-Ingenieure dürfte mit Design, Programmierung, Test und Integration eingebetteter Computersysteme beschäftigt sein. Üblicherweise arbeiten diese Systeme unter Echtzeitbedingungen und engen Vorgaben, was den Stromverbrauch angeht. Mehr Performance und eine flexible Architektur sind nicht nur für eine bequeme Benutzung nötig, sondern auch für eine Verlängerung der „Produktlebenszeit“. Gleichzeitig steigt die Komplexität dieser Systeme exponentiell bei ständigem Druck, die Zeit bis zur Marktreife zu verkürzen.

Obwohl die Halbleitertechnik in naher Zukunft eine Milliarde Transistoren pro Quadratzentimeter verbauen kann, bleibt die Frage, wie gut die Designer diese Entwicklung nutzen können. Produktivitätsverbesserungen sind und bleiben eine zentrale Aufgabe der Entwickler.

High-Level-Synthese ist in diesem Zusammenhang ein wichtiger Ansatz. Eine frühe Systemoptimierung auf hoher Abstraktionsebene kann zusammen mit nach verschiedenen Kriterien (Laufzeiten, Flächenbedarf) optimierenden Synthesewerkzeugen diese einander widersprechenden Anforderungen unter einen Hut bringen. So sind signifikante Verbesserungen der Qualität des gesamten Systems möglich [1]. Der wichtigste Hebel der Optimierung, auch auf hohem Abstraktionsniveau, ist die frühe und effiziente Nutzung aller Designbeziehungen. Durch die Nutzung von High-Level-Tools lässt sich hier eine deutlich bessere Performance erreichen, abgesehen von geringeren Kosten und weniger Stromverbrauch.

Richtig modellieren

Einer der ersten Schritte ist die Modellierung des Systems durch abstrakte Beschreibungssprachen wie UML, SDL oder Programmiersprachen wie C/C++ und Java. Die Funktion des Systems kann so verifiziert werden, und man hat eine gute Chance, mögliche Performance-Engpässe zu identifizieren. Leider lassen sich in den meisten aktuell genutzten Sprachen nichtfunktionale Bedingungen wie Performance und Stromverbrauch nicht abbilden.

Das führt zu einem wachsenden Bedarf an High-Level-Synthese-Werkzeugen zur Verarbeitung von abstrakten Beschreibungen, die sich während des Designprozesses verändern lassen. So könnte man ein komplettes Design in Hard- und Software generieren lassen, das mit kommerziellen Tools kompiliert und gleichzeitig simuliert werden kann. Design Space Exploration oder ein signifikanter Teil davon steht für diese Tools ebenfalls auf der Wunschliste.

Nach unseren experimentellen Erfahrungen kann der Einsatz von High-Level-Synthese-Tools den Design-Zyklus neuer Produkte entscheidend verkürzen; besonders in rechenintensiven Anwendungen. Manche Werkzeuge wie Catapult C (Mentor Graphics) und der C2H-Compiler (Altera) können eine Teilmenge von ANSI-C respektive C++ direkt in HDL (Hardware Description Language) übersetzen, etwa in VHDL (Very High Speed Integrated Circuit Hardware Description Language) oder Verilog.

Diese und ähnliche Tools analysieren zunächst, ob sie alle Datenstrukturen und -typen im Quellcode „verste-

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

hen“. Der Benutzer muss den Code nicht nur dahingehend verändern, sondern auch so, dass das ausgewählte Werkzeug in der Lage ist, effizientere Design-Alternativen zu generieren. Je nach Tool wird dann das Design mithilfe von gelegentlichen Benutzereingriffen schrittweise verfeinert.

Zu diesem Zweck bietet beispielsweise Catapult C viele Benutzeroptionen zur weiteren Designoptimierung. Gleichzeitig wird werkzeugabhängig durch ausgewählte Strukturen oder Programmtricks ein effizienteres Designs erzeugt, insbesondere bei der Optimierung von Schleifen und Speichermapping-Strukturen.

Daher ist die Erfahrung des Anwenders mit dem Tool und in Sachen Hardwaredesign ein entscheidender Faktor. Schlechte Ergebnisse haben oft mehr zu tun mit einer unsachgemäßen Auswahl der Werkzeuge, der Unfähigkeit zur Nutzung der verfügbaren Optimierungsoptionen oder Qualitätsmängeln des Ausgangscodes als mit dem Werkzeug selbst.

Einige Werkzeuge wie der C2H-Compiler setzen voraus, dass der ursprüngliche Quellcode auf einer bestimmten Plattform, in diesem Fall Alteras NIOS-Prozessor, lauffähig sein muss, bevor sie ihn weiterverarbeiten. Das Tool kann dann aus dem ursprünglichen Quelltext ein hardwarebeschleunigtes System entwerfen. Der Benutzer kann entscheiden, performancekritische Funktionen aus der Software in die Hardware zu verlegen und im FPGA (Field Programmable Gate Array) zu implementieren. Die dazu nötige Hardware-Software-Schnittstelle generiert das Tool, das neu auf Hardware und Software verteilte System läuft dann auf einem NIOS-basierten Modul.

Zwar sind solche Werkzeuge auf bestimmte Plattformen beschränkt, doch das ermöglicht ihnen, die Schnittstelle zwischen der erzeugten HDL-Beschreibung und dem restlichen Teil der Software selbst zu generieren. Dennoch sollte man, um hochwertige Design-Alternativen zu erhalten, vorab den Sourcecode entsprechend den Anforderungen des Werkzeugs ändern. Manchmal muss der Benutzer den Quelltext mehrmals modifizieren, um verschiedene Optimierungstechniken zu nutzen, die das Tool zum Entwurf von Design-Alternativen veranlassen. Das ermöglicht explizite Vergleiche der unterschiedlichen Designvorgaben, was etwa die Erkundung des Design Space oder von Teilen davon angeht. Je mehr Alternativen er analysiert, desto sicherer kann der Entwickler sein, sich mit seiner gewählten Konstruktion dem Optimum weitestmöglich genähert zu haben. Catapult C zum Beispiel kann automatisch alle generierten Alternativen vergleichen und die Ergebnisse dem Anwender in verschiedenen Formen präsentieren.

iX-TRACT

- High-Level-Synthese-Tools sollen den Entwicklungszyklus verkürzen und die Qualität des Designs verbessern helfen.
- Viele Anwendungen des Embedded Computing sind zu komplex, um ohne individuelle Anpassungen optimal zu funktionieren.
- Als wichtige Vorgehensweise hat sich das Co-Design erwiesen, die gleichzeitige Entwicklung von Hard- und Software.

Doch in vielen Anwendungsbereichen, etwa komplexen Steuersystemen, liefern High-Level-Synthese-Tools oft schlechtere Ergebnisse als erwartet. Für solche Anwendungen ist ein tiefes Verständnis der Algorithmen und der Erwartungen an die Arbeitsumgebung erforderlich. Normalerweise werden performancekritische Abschnitte anhand einer gründlichen Analyse unter Berücksichtigung verschiedener Szenarien bestimmt. Daraus lässt sich dann die geeignete Technik zur Beschleunigung bestimmen, die nicht unbedingt hardwarebasiert sein muss. In vielen Fällen ist eine Softwareänderung das – auch deutlich kostengünstigere – Mittel der Wahl.

Effizient kombinieren

Nach unseren Erfahrungen führt vor allem die effiziente Kombination von Software- und Hardwarebeschleunigung, im Sinne des sogenannten Co-Designs, zum günstigsten Preis-Leistungs-Verhältnis. In frühen Designschritten lassen sich komplexe Algorithmen analysieren und so weit wie möglich vereinfachen, hinsichtlich mehr Regelmäßigkeit, weniger Kommunikation zwischen funktionalen Blöcken, Ersetzen komplexer Operationen und so weiter.

Die Vereinfachung von Algorithmen ist ein wichtiger Schritt, nicht nur in anwendungsspezifischen Anpassungen, sondern auch beim Einsatz von High-Level-Synthese-Tools. Zudem kann diese Vereinfachung die Komplexität der Hard-/Software-Schnittstellen reduzieren. In diesem Zusammenhang sei erwähnt, dass hardwarebasierte Performanceverbesserung entweder als separater Beschleunigungs-Chip, neben dem Prozessor, umgesetzt werden kann oder in Form benutzerdefinierter Anweisungen (unter NIOS-Systemen). Benutzerdefinierte Anweisungen erweitern den Befehlssatz des Prozessors oder seine Architektur.

Ein typischer Syntheseprozess stellt sich als eine Reihe aufeinander folgender Optimierungsschritte dar. Dazu hat jedes High-Level-Synthese-Tool seinen eigenen Optimierungsalgorithmus, der die Qualität der erzeugten Design-Alternativen bestimmt sowie die erforderliche Zeit, um eine Alternative im Rahmen der vorgegebenen Bedingungen zu finden.

High-Level-Synthese auf einen Blick

Man kann High-Level-Synthese als Transformation einer Verhaltensbeschreibung eines Designs in eine Register-Transfer-Beschreibung (RTL: Register Transfer Language) betrachten. Die Art der Beschreibung des Systemverhaltens hängt von der Entwicklungsumgebung ab. Üblich sind Grafiken oder Modelle in Programmiersprachen wie C/C++. Grundsätzlich besteht der Syntheseprozess aus drei Hauptschritten: Allocation (Zuweisung der Ressourcen), Binding (Zuweisung der Aufgaben) und Scheduling (Ablauf).

Die Zuweisung der Ressourcen bestimmt Art und Anzahl der Instanzen der einzelnen grundlegenden Hardwarekomponenten, die zur Umsetzung eines Algorithmus erforderlich sind. Der Syntheseprozess in Automatisierungs-Tools stellt Komponenten aus Bibliotheken zusammen, die in der Regel zum Lieferumfang gehören. In vielen kommerziellen Tools wie Catapult C lassen sich diese Bibliotheken durch den Designer um individuelle, speziell optimierte Komponenten erweitern. Empfehlenswert sind unterschiedliche Typen der gleichen Komponente, zum Beispiel eine optimiert für Leistung und eine andere für Energieverbrauch.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Während des Bindens werden Operationen oder Aufgaben des Algorithmus den Hardwarekomponenten zugewiesen, sodass jeder Aufgabe jederzeit eine Hardware-Instanz zugeordnet ist.

Catapult C beispielsweise erlaubt dem Entwickler, eine Ressource an eine bestimmte Art von Hardwarekomponente zu binden und festzulegen, wie sie physikalischem Speicher zugeordnet ist. Der Entwickler hat durch Ressourcenbegrenzungen die Kontrolle darüber, welche Komponenten für welche Operationen reserviert sein sollen. Er kann so die Art und Weise beeinflussen, wie das Design in verschiedenen Stufen verfeinert wird.

Das Scheduling-Verfahren bestimmt die Reihenfolge der Ausführung nach den gegebenen Zuweisungen, sodass die zeitliche Durchführbarkeit gewährleistet ist. Dies wird üblicherweise durch Gantt-Diagramme dargestellt. Catapult C erzeugt diese automatisch, um dem Anwender das Timing-Verhalten des Systems anschaulich zu demonstrieren.

Zur Verbesserung der Designqualität ist der Benutzer gehalten, die Ergebnisse von High- Level-Synthese-Tools nach jedem Schritt zu analysieren. Zum Beispiel die Untersuchung der von Catapult C automatisch generierten Gantt-Diagramme kann in mehreren Fällen dem Benutzer helfen, die Architektur- und /oder Ressourcen-Einschränkungen (constraints) besser abzustimmen. Diese ersten Ergebnisse können Quellcode-Änderungen erforderlich machen, um das eine oder andere Designziel besser zu realisieren. In Catapult C wird der Benutzer aufgefordert, verschachtelte C-Schleifen mit festen Grenzwerten für jeden Loop zu versehen. Dies erleichtert dem Tool die Optimierung der Schleifen.

Praktische Beispiele

Eine bemerkenswerte, wichtige Eigenschaft aller High-Level-Synthese-Tools ist die relativ kurze Zeit, die sie verglichen mit traditionellen Designmethoden zum Generieren und Evaluieren von Design-Alternativen benötigen. Dennoch ist die Erfahrung der Designer ein wichtiger Faktor, der keinesfalls ignoriert werden darf. Wie auch immer, wer anwendungsspezifische Hardwarebeschleunigung in Erwägung zieht, sollte auf jeden Fall zuvor die beschriebenen Syntheseschritte durchgeführt haben.

Nun zu einigen Fällen anwendungsspezifischer Hard-/Software-Beschleunigungs-Techniken. Obwohl der Autor in vielen Anwendungsbereichen mit High-Level-Synthese arbeitet, konnte in den hier betrachteten Fallstudien keines der vorgestellten Werkzeuge einen bemerkenswerten Vorteil erzielen. Das hängt insbesondere mit der Komplexität der Algorithmen zusammen. Ein Synthese-Tool-gerechtes Umschreiben wäre deutlich aufwendiger als eine Neuprogrammierung.

Das erste Beispiel ist die Java-Implementierung von MP3, als Teil des Multi-Standard-Audio-Systems (SDMA). Im zweiten Beispiel, dem RSA-Kryptografie-Algorithmus, wird dieser durch spezielle Hardware beschleunigt.

Java-Anwendungen für MP3 wurden ursprünglich von JavaZOOM im JLayer-Projekt entwickelt [2]. JLayer stellt eine Java-Bibliothek zur Verfügung, die MP3-Sound-Dateien dekodiert, konvertiert und in Echtzeit abspielt. Es unterstützt die MPEG-Layer 1, 2 und 3. In der Regel ist eine Java-MP3-Implementierung auf Desktop-Computern keine große Herausforderung, da schnelle Prozessoren verfügbar sind. Im Gegensatz dazu steht eine Echtzeit-Dekodierung auf eingebetteten Plattformen wie NIOS schnell vor Performanceproblemen. Einen entscheidenden Einfluss auf die Gesamtleistung der Java-Applikation hat die Java Virtual Machine (JVM), eine Software-Implementierung eines „Prozessors“, der architekturneutrale Anweisungen auf einem realen Prozessor ausführt.

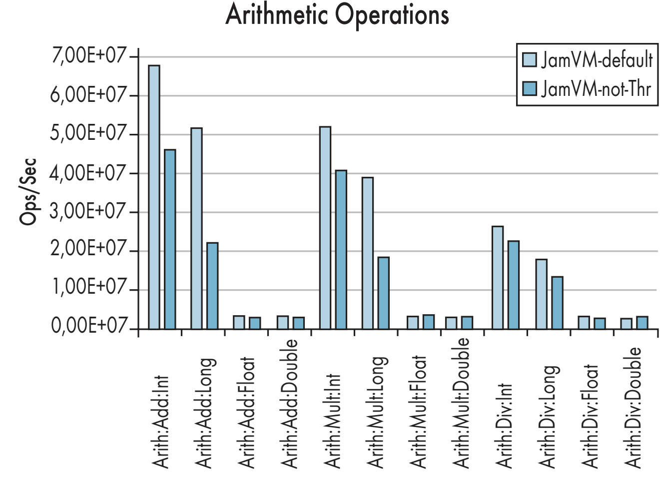
Die Performance der Robert-Lougher-JamVM wurde eingangs mit verschiedenen Benchmarks der Java-Benchmark-Suite Grande [3] gemessen. Vor individuellen Anpassungen auf der Anwendungsebene ging es erst einmal darum, die Unterschiede zwischen der threaded und switched (umgeschalteten) Implementierung der JVM festzustellen (Abbildung 1).

Ergebnis: Der Umstieg von Task-Wechseln auf Threads kann die Verarbeitungsgeschwindigkeit verdoppeln. Einschränkend sei gesagt, dass dieses Ergebnis nur für arithmetische Operationen gilt. Eine ebenfalls drastisch verbesserte Performance erzielt der Wechsel vom Interpreter- in den Compiler-Modus der JVM. Bei Letzterem werden Teile des Codes übersetzt und dann ohne zwischengeschaltete JVM direkt als Maschinencode ausgeführt. Der Unterschied zwischen den JVM-Versionen von Sun und der JamVM, Letztere mit GNU Classpath, ist dagegen kaum messbar. Referenzsystemplattform war ein Linux-Rechner mit 3-GHz-Prozessor und 2 Gigabyte RAM.

Mindestens ebenso wichtig kann natürlich die Beschleunigung der einzelnen Softwareteile sein. Bei der MP3-Kodierung erfolgte dies durch Profiling und bekannte Verfahren wie das Verlagern oft aufgerufener Unterprogramme in Inline-Code. Typischer für das Zusammenspiel von Soft- und Hardware bei Embedded Systems sind aber die bei der RSA-Verschlüsselung durchgeführten Schritte, die darum hier im Einzelnen erörtert werden.

RSA Beine machen

Der ursprüngliche RSA-Algorithmus ist in Java entwickelt und arbeitet daher relativ langsam. Beschleunigungstechniken sollten die Performance der gesamten Anwendung verbessern. So können zur Beschleunigung ausgewählte Teile des Algorithmus in nativen Code umgesetzt werden. Durch Hardwarebeschleunigung via FPGA dagegen lassen sich sowohl die Sicherheit als auch die Leistung verbessern. Wo rechenintensive Abschnitte des Algorithmus auf die Hardware migriert werden, sollte ein Hard-Software-Co-De-



Doppelt so schnell durch Threading: Performance-Unterschiede zwischen den unterschiedlichen Implementierungen der JamVM (Abb. 1)

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Java-Tempo

JVM	Modus	ms/Frame	Zeit (ms)
Sun JVM	interpretiert	11	5104
Sun JVM	kompiliert	3	1450
JamJVM	interpretiert	11	5050

Kompilieren statt interpretieren ist fast 4 × schneller.

sign weitere Optimierungen ermöglichen. Neben der Leistungsverbesserung ist es bei dieser Migration wichtig, den durch die Teilauslagerung auf die Hardware erzeugten Kommunikationsaufwand in Grenzen zu halten. Der Rest der Anwendung läuft wie zuvor in Software.

JNI als Hard-Software-Brücke

Software und neu entwickelter Hardwarebeschleuniger kommunizieren über das Java Native Interface (JNI). Der Beschleuniger ist direkt in einer Hardwarebeschreibungssprache entwickelt und wird mithilfe des ALTERA SOPC-Builders (SOPC steht für System On a Programmable Chip) in die eigentliche Anwendung eingebunden. Zwar haben Experimente erwiesen, dass JNI eine Quelle verschiedener Performance-Einbußen sein kann. Doch ein sauberes Co-Design des ganzen Systems kann diesen Einfluss auf ein normales Maß reduzieren.

Kern des RSA-Algorithmus ist das modulare Potenzieren, eine Kombination aus Potenzieren und Modulo-Operationen. Um zum Beispiel das n-Bit-Wort X in das Wort Y=enc(X) zu verschlüsseln, wird folgende Funktion benutzt:

$Enc(X)=\langle X^E\rangle_M$, wobei E der Schlüssel oder der öffentliche Exponent ist und M der Modulus. Zur Verringerung der Komplexität wird der RSA-Algorithmus auf der Grundlage des Montgomery-Algorithmus berechnet, der eine effiziente Möglichkeit zur Umsetzung der modularen Multiplikation ohne die Notwendigkeit eines aufwendigen Hardwareteilers bietet [4]. Statt der Division kommen nur Schiebeoperationen zum Einsatz, ein entscheidender Optimierungsfaktor. Dieses Weniger an Komplexität minimiert den erforderlichen Hardwareaufwand.

Der Kern des Montgomery-RSA-Algorithmus ist in Hardware (FPGA) implementiert, mit einem Multiplizierer und einem Quadrierer (Abbildung 2). Zudem sind zwei zusätzliche parallele und ein serielles Register erforderlich.

Listing für RSA-Algorithmus

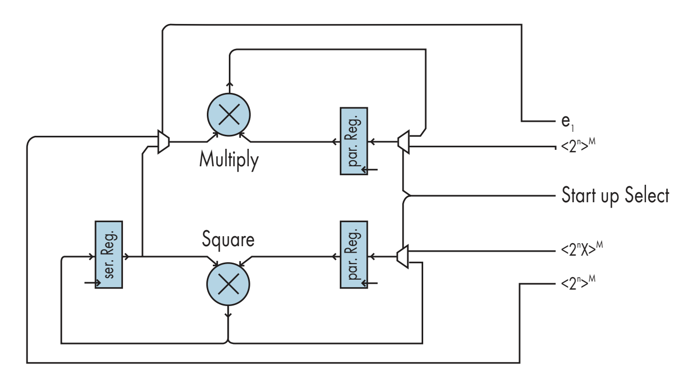
```
@lf:public class RSA{
      private final static BigInteger bI   = new BigInteger("1");
      private final static SecureRandom sR = new SecureRandom();
      private BigInteger privateKey;
      private BigInteger publicKey;
      private BigInteger modulus;

RSA (int Rand){
BigInteger P  = pPrime (Rand/2, sR);
BigInteger Q  = pPrime (Rand/2, sR);

publicKey                 = getPulicKey(P, Q);
privateKey                = getPrivateKey(P, Q);
BigInteger  modulus       = getModulus(P, Q);
}

     Public BigInteger[] encrypt(BigInteger[] word) {
         BigInteger[] pWord = preProcess (BigInteger[] word);
         BigInteger[] message = encryptMessage (pWord,modulus,P);
         return message;
     }
     /* native call*/
     public static native BigInteger[] encrypt (Message
                         BigInteger[] pWord,
                         BigInteger modulus BigInteger P);
}
```

Beispielhafte Java-API: der Hardwarebeschleuniger für den RSA-Montgomery-Algorithmus



Schematische Ansicht des angepassten Beschleunigers für den RSA-Montgomery-Algorithmus (Abb. 2)

Beim Start werden die Skalierungsfaktoren in die parallelen Register geladen. Um den durch den Montgomery-Algorithmus erzeugten 2^n-Effekt aufzuheben, ist eine abschließende Multiplikation mit 1 erforderlich. Der Rest der Anwendung ist in Java implementiert, inklusive der erforderlichen APIs für den Zugriff auf den Hardwarebeschleuniger. Einen Ausschnitt zeigt das Listing.

Fazit

Bei der Entwicklung eingebetteter Systeme sind trotz des bemerkenswerten Entwicklungsstands von High-Level-Synthese-Tools individuelle Anpassungen immer noch unabdingbar. Eine frühzeitige Optimierung mit dem Ziel der Reduzierung der Komplexität ist ein Schritt, der sowohl zur anwendungsspezifischen Optimierung nötig ist als auch zu der durch High-Level-Synthese-Tools. Wichtig bei der individuellen Optimierung ist der Co-Design-Ansatz, die gleichzeitige Betrachtung von Hard- und Software: Nach der Aufteilung der Anwendung kann man die Hardware co-entwickeln, zur Verbesserung der Leistung des Gesamtsystems.

Den Softwareteil, der so kompliziert sein kann wie eine JVM, sollte man je nach Bedarf optimieren, wie die erste Fallstudie zeigt. Im Licht der Experimente relativieren sich auch die potenziellen Vorteile der High-Level-Synthese. So hilfreich diese für die Steigerung der Entwicklerproduktivität ist, ersetzt sie nicht die individuelle, anwendungsspezifische Anpassung. Erst der richtige Mix aus beiden Methoden kann die vielfältigen, oft gegensätzlichen Erfordernisse komplexer Applikationen erfüllen. (JS)

AMJAD MOHSEN

arbeitet am Fraunhofer Institute for Integrated Circuits IIS an der Optimierung integrierten Hard-Software-Co-Designs.

Literatur

[1] A. Mohsen, R. Hofmann; Efficient Voltage Scheduling and Energy-aware Co-synthesis for Real-time Embedded Systems; 10th Asia-Pacific Computer Systems Architecture Conference (ACSAC 05); Singapur, 24.-26. Oktober 2005

[2] The JLayer Project; www.javazoom.net

[3] The Java Grande Forum Benchmark Suite; www2.epcc.ed.ac.uk/computing/research_activitie/java_grande/

[4] C.D. Walter; Montgomery Exponentiation Needs no Final Subtraction; Electronic letters online; 1999, 35, pp. 1832-1833.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Java-Code für Multi-Core-Umgebungen schreiben

Kernig kodiert

Nils Gruschka, Luigi Lo Iacono, Jörg Wagner



Auf Multi-Core-Systemen können parallelisierte Algorithmen deutliche Geschwindigkeitsvorteile bringen. Dass mehr Kerne nicht zu einer linearen Temposteigerung führen, ist jedoch nur eine der in diesem Umfeld zu nehmenden Hürden.

Bis heute ist die Welt der Parallelverarbeitung die Domäne einiger weniger Spezialisten, die sich auf die Implementierung nebenläufiger Algorithmen verstehen. Meist bearbeiten die hierbei entwickelten Programme komplexe numerische Aufgaben, die beispielsweise die Grundlage für Crashtest-Simulationen oder Wetterprognosen bilden. Für ihre Lösung geeignete System sind bis dato oft in spezialisierten Rechenzentren anzutreffen. Die Etablierung von Mehrkern-Prozessoren in PCs oder eingebetteten Systemen weicht diese Grenze auf und lässt Großrechner-Technik auf den Schreibtisch wandern. Dies bedingt, dass Parallelverarbeitung in herkömmliche (sequenzielle) Software einziehen muss, damit man die Leistungsfähigkeit von Mehrkern-Systemen ausnutzen kann. Im Folgenden geht es darum, was dies für Java-Programmierer bedeutet.

In den vergangenen 30 Jahren bestimmte das Mooresche Gesetz die Leistungssteigerung von Rechnern. In Zukunft wird sie allerdings stärker vom Amdahlschen Gesetz geprägt sein (siehe den gleichnamigen Kasten). Es besagt, dass das theoretisch erzielbare Leistungsplus mit steigender Prozessoranzahl immer stärker vom sequenziellen Anteil der Anwendung abhängt. Um es ausschöpfen zu können, ist die durchgängige Parallelisierung also eine zwingende Voraussetzung. Bei Java-Software sind mehrere Schichten bezüglich ihrer Parallelisierbarkeit zu betrachten, beginnend bei der JVM über die zugrunde liegenden (Laufzeit-)Bibliotheken bis hin zur Anwendung selbst.

Java bot von Anfang an Parallelisierungsmöglichkeiten. Dazu gehört als integraler Sprachbestandteil der Thread, mit dem sich Teile des Codes parallel ausführen lassen. Die JVM befreit den Entwickler von der Aufgabe, Threads auf Prozesse des Betriebssystems abzubilden und damit auf verschiedene Prozessorkerne zu verteilen. Wie dies im Detail stattfindet, wurde zudem bewusst aus den Spezifikationen der JVM ausgespart, um Freiraum für die unterschiedlichen Eigenschaften der verschiedenen Betriebssysteme zu wahren. Dies ist einer der Gründe für unterschiedlich effiziente JVM-Implementierungen.

Den Speicher richtig aufräumen

Automatische Speicherbereinigung (Garbarge Collection, GC) ist eine wichtige Funktion von Java. Sie gibt den Speicher nicht mehr benötigter Objekte automatisch wieder frei und befreit damit den Entwickler von dieser mühseligen Aufgabe. Auch für die automatische Speicherbereinigung stellen Mehrkern-Systeme eine Herausforderung dar. So verbraucht eine Applikation, die 1% ihrer Laufzeit für GC verwendet, auf einem System mit 32 Kernen bereits ein Viertel der Gesamtlaufzeit dafür (siehe Kasten zum Amdahlschen Gesetz). Neuere Versionen der JVM lockern diese Bremse durch parallele GC-Algorithmen.

Dazu gehören der durch *-XX:+UseParallelGC* aktivierte „Throughput Collector“ und der „Concurrent Low Pause Collector“, den *-XX:+UseConcMarkSweepGC* einschaltet. Der Throughput Collector ist besonders geeignet für Applikationen, die viele Objekte erzeugen (das heißt eine große Population in der Young Generation haben) und der Con-

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Listing 1: Intuitiver Ansatz zur Parallelisierung des Miller-Rabin-Test

```
int cpuCount = Runtime.getRuntime().availableProcessors();
ExecutorService pool = Executors.newFixedThreadPool(cpuCount);
do {
  // Wähle zufälliges n
  ArrayList<TestPrime> primeTesters = new ArrayList<TestPrime>();
  for (int t = 0; t < 100; t++) {
    // Wähle zufälliges a
    primeTesters.add(new TestPrime(n,a));
  }
  testResults = pool.invokeAll(primeTesters);
} while(!checkResults(testResults));
...
class TestPrime implement Callable {
  public Boolean call() {
    return witness(n,a);
  }
}
```

Das Amdahlsche Gesetz

$$S = \frac{1}{(1 - P) + P/N}, \text{ wobei}$$

S: Gesamtbeschleunigung
P: Anteil der Anwendung, die sich parallelisieren lässt
N: Anzahl der Prozessoren

Verbringt das Programm etwa 1% seiner Laufzeit mit sequenziellen Aufgaben (P=99/100) und läuft es auf 32 Prozessoren, ist S ungefähr 24. Gegenüber der vollständigen Parallelisierung, bei der S=32 wäre, entfallen also rund 8/32 auf den sequenziellen Teil – ein Viertel der Gesamtlaufzeit. Doppelt so viele CPUs treiben S auf 39 hoch, und auf den sequenziellen Teil entfallen in diesem Fall 25/64, also fast 40 %.

current Low Pause Collector für solche Applikationen mit langlebigen Objekten (das heißt einer großen Population in der Tenured Generation). Testläufe mit verschiedenen Kollektoren helfen, den für das jeweilige Projekt geeigneten zu finden. Hierfür liefert die JVM, angewiesen durch

```
-verbose:gc -XX:+PrintGCDetails \
 -XX:+PrintGCTimeStamps
```

Daten, die man mit Tools wie VisualGC und JConsole (auch visuell) auswerten kann (s. *iX*-Link). Vor der Wahl eines anderen GC sollten weitere Tuning-Möglichkeiten wie die Änderung der Größe des Heap-Speichers (*-Xms -Xmx*) oder der Generationen (*-Xmn -XX:NewSize -XX:MaxNewSize*) ausgeschöpft sein [1].

Bibliotheken bilden für die meisten Entwickler die ideale Stelle, an der sich der Programmcode den aktuellen Prozessorentwicklungen anpassen sollte. Für viele Aufgaben lässt sich hier unter Beibehaltung des Interface ein paralleler Programmablauf implementieren. Gerade Anwendungen, die die meiste Zeit in (Standard-)Bibliotheken verbringen, profitieren auf einen Schlag von Verbesserungen – ohne dass Code-Änderungen nötig wären.

Bibliotheken parallelisiert

Beispiele hierfür sind Bibliotheken für Kryptografie oder Lineare Algebra. Auch die Java-Klassenbibliothek beinhaltet enormes Potenzial zur besseren Ausnutzung von Mehrkern-Systemen durch parallele Algorithmen. Die aktuelle Implementierung von *Collection.sort()* im Java Collection Framework (JCF) ist beispielsweise sequenziell realisiert. Initiativen zur Parallelisierung des JCF gab es bereits vor einigen Jahren im Java Community Process JSR-166 (s. *iX*-Link). Ergebnisse hieraus sind inzwischen in das Paket *java.util.concurrent* (ab Java 5) eingeflossen, und der Prozess der Integration paralleler Algorithmen in die Java-Standardbibliothek schreitet weiter voran. So wird das kommende Java 7 unter anderem Implementierungen zum parallelen Suchen und Sortieren von Datenfeldern enthalten.

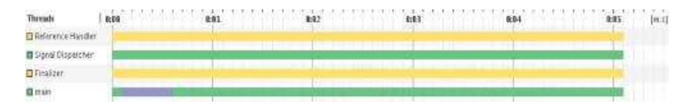
Bedingt durch den geringen Komfort und die hohe Komplexität – insbesondere beim Beseitigen von Hürden wie Race-Conditions und Deadlocks – hält sich die Verwendung und Verbreitung von Threads stark in Grenzen und ist außerhalb der GUI-Programmierung kaum anzutref-

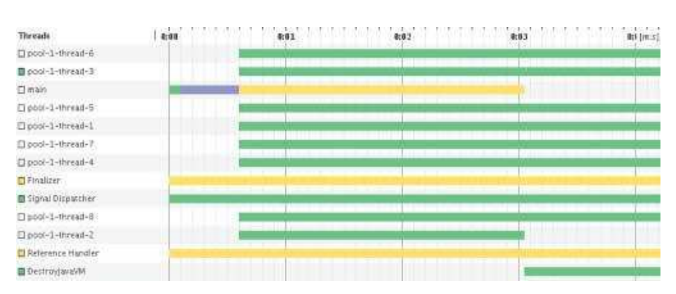
iX-TRACT

- Multi-Core-Systeme lassen sich durch parallelisierte Java-Programme besser nutzen, sodass sie schneller laufen.
- Vorteile durch Parallelisierung können Entwickler in der Java-VM etwa durch Wahl eines passenden Garbage Collectors erreichen.
- Von nebenläufigen Algorithmen in Bibliotheken, beispielsweise zum Sortieren, profitieren alle Anwendungen.
- Das Parallelisieren der Anwendung selbst erfordert eine genaue Untersuchung des verwendeten Algorithmus, denn ungeschicktes Vorgehen kann ihn sogar verlangsamen.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.





Mit dem in Netbeans integrierten Profiler lassen sich Threads visualisieren (links für die sequenzielle, rechts für die parallele Implementierung des Rabin-Miller-Tests). Grüne Balken stehen für laufende, gelbe und violette für wartende Threads.



fen. Bei J2EE verwendet man sogar gezielt ein sehr einfaches Thread-Modell, das Entwicklern die Arbeit erleichtern soll. Eine goldene Designregel besagt beispielsweise, dass Servlets oder EJB keine Threads erzeugen sollten, damit das Threading exklusiv unter der Kontrolle des Web-Applikationsservers verbleibt. Einen Kompromiss bildete der Application Server Work Manager [2], der Entwicklern Methoden zur Implementierung nebenläufiger Web-Applikationen an die Hand gab und dem Server dennoch die Kontrolle über die Threads beließ. Dieses Projekt ist inzwischen eingestellt.

Alternativen für Parallelisierung

Aufgrund dieser nicht auf Java beschränkten Schwierigkeiten beim Verwenden von Threads haben sich in den letzten Jahren alternative Ansätze für parallele Algorithmen auf SMP-Systemen etabliert, darunter die daten- und die aufgabenorientierte Parallelisierung. Datenparallele Verarbeitung ist dadurch gekennzeichnet, dass derselbe Algorithmus gleichzeitig auf unabhängigen Eingabedaten läuft, meist mit der Einschränkung, exakt dem gleichen Programmfluss zu folgen. Die aufgabenorientierte Parallelisierung entspricht dagegen „Threads auf Miniaturebene“. Neben dem Verstecken der Thread-Komplexität hinter einer höheren Abstraktion geht es darum, die Aufgabe in möglichst viele unabhängige Teile (Tasks) zu zerlegen, die auf beliebig vielen Prozessorkernen laufen. Dabei gilt es jedoch, eine gewisse Größe der Tasks nicht zu unterschreiten, damit sich der durch ihr Erzeugen, Verwalten und Synchronisieren erzwungene Overhead in Grenzen hält. Viele kleine, unabhängige Tasks sichern eine gewisse Skalierbarkeit auf zukünftigen Systemen ebenso wie eine gleichmäßige Lastverteilung auf die CPUs. Des Weiteren erledigt die Applikation eigenständig die Tasks, während sie der JVM beziehungsweise dem Betriebssystem nur eine überschaubare Anzahl aktiver Arbeitsthreads präsentiert.

Die einfachste Form eines solchen Schedulers ist ein Pool von Threads, die parallel eine Liste wartender Tasks abarbeiten. Ein solches Verfahren zog mit Java 5 in den Standard ein. Seine Verwendung illustriert hier der Rabin-Miller-Test [3]. Er ist einer der wichtigsten Algorithmen zum Testen großer Zahlen auf die Eigenschaft „prim“. Es handelt sich um ein probabilistisches Verfahren, dessen Ergebnis nur mit einer gewissen Wahrscheinlichkeit korrekt ist. Durch mehrfache Wiederholung des Tests kann man die Wahrscheinlichkeit einer Falschaussage so weit reduzieren, dass sie für praktische Belange Null ist.

Im Wesentlichen funktioniert der Rabin-Miller-Test folgendermaßen: Zunächst wählt man zufällig eine Zahl *n* als Primzahlkandidaten. Danach prüft der Algorithmus für eine zufällig zwischen *2* und *n-1* gewählte Zahl *a*, ob sie ein sogenannter „Belastungszeuge“ dafür ist, dass *n* eine Primzahl ist (s. Kasten „Der Rabin-Miller-Test“).

Wahrscheinlich eine Primzahl

Ist das Ergebnis falsch, kann dieses *n* keine Primzahl sein; es kommt ein neues ins Spiel. Ein wahres Resultat erhöht die Wahrscheinlichkeit, dass *n* eine Primzahl ist, und der Text wird für einen weiteren Zeugen *a* ausgeführt. Diesen Schritt wiederholt man bis zu einer vorher bestimmten Grenze (beispielsweise 100). Fällt auch der letzte Test positiv aus, darf *n* mit hoher Wahrscheinlichkeit als Primzahl gelten.

Zur Parallelisierung bieten sich bei diesem Algorithmus zwei Ansatzpunkte an. Da zum Finden einer einzigen Primzahl eine große Menge von Kandidaten nötig ist, kann ihre Erzeugung parallel stattfinden. Weiterhin lassen sich für jeden Kandidaten die Zeugentests gleichzeitig ausführen. Listing 1 zeigt den (vereinfachten) Programm-

Der Rabin-Miller-Primzahltest

Der folgende Algorithmus testet, ob eine natürliche Zahl n nach dem Rabin-Miller-Verfahren eine Primzahl ist:

1. Wiederhole 100-mal:

1.1 Wähle $a \in \{2$ und n-1$\}$

1.2 Wenn `witness`(n, a)=FALSCH: Abbruch; *n* ist keine Primzahl

2. *n* ist Rabin-Miller-prim

Der dabei verwendete Zeugentest `witness`(n, a) ist wie folgt definiert:

1. Wähle $u, t \in \mathbb{N}$ mit u ungerade und $2^t u = n - 1$

2. Überprüfe, ob gilt: $a^u \equiv 1 \bmod n$

3. Überprüfe, ob gilt: es gibt ein $0 \le r \le t$ mit: $a^{u \cdot 2^r} \equiv -1 \bmod n$

4. Falls 2 ODER 3 erfüllt Ergebnis: WAHR, sonst Ergebnis: FALSCH

Listing 2: Optimierter paralleler Rabin-Miller-Test

```
int cpuCount = Runtime.getRuntime().availableProcessors();
ExecutorService pool = Executors.newFixedThreadPool(cpuCount);
do {
  ArrayList<CreatePrime> primeGen = new ArrayList<CreatePrime>();
  for (int c = 0; c < cpuCount; c++) {
    primeGen.add(new CreatePrime());
  }
  n = pool.invokeAny(primeGen);
  ArrayList<TestPrime> primeTesters = new ArrayList<TestPrime>();
  for (int t = 0; t < 99; t++) {
    // Wähle zufälliges a
    primeTesters.add(new TestPrime(n,a));
  }
  testResults = pool.invokeAll(primeTesters);
} while(!checkResults(testResults)
...
class CreatePrime implement Callable {
  public BigInteger call() {
    do {
      // Wähle zufälliges n und a
    } while(!witness(n,a));
  }
}
```


© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

code, der den Zeugentest mit einem Java-Thread-Pools parallelisiert. Er bekommt eine Liste von „Aufträgen“ in Form von Objekten übergeben, die das *Callable*-Interface implementieren. Hier sind dies Objekte der Klasse *TestPrime*, die bei Aufruf den Zeugentest für ein *n* und ein *a* ausführen.

Dieser intuitive Ansatz zur Parallelisierung des Rabin-Miller-Tests führt zu einem unerwarteten Ergebnis: Er ist deutlich langsamer als eine sequenzielle Umsetzung. Eine Analyse des Laufzeitverhaltens enthüllt schnell den Grund: Die Anzahl der für ein *n* befragten Zeugen ist nicht über den Bereich von 1 bis 100 gleichverteilt. Fast immer findet nur ein Test eines oder aller 100 Zeugen statt, weil entweder nach dem ersten bewiesen ist, dass *n* keine Primzahl ist, oder *n* ist Rabin-Miller-prim. Denn die Wahrscheinlichkeit, dass eine zusammengesetzte Zahl auch nur einen Zeugentest besteht, geht für große *n* gegen 0. So zeigen Damgård und seine Kollegen in [4], dass sie für 600 Bit lange Zahlen bereits kleiner als 2^{-75} ist.

Die vorgestellte parallele Implementierung startet deshalb in vielen Fällen zu viele Zeugentests. Ein verbesserter Algorithmus führt daher den ersten Zeugentest sequenziell nach der Wahl von *n* durch und die restlichen 99 wie oben parallel. Listing 2 zeigt die verbesserte Variante mit einer parallelen Erzeugung von Primzahlkandidaten. Auf einem System mit acht Prozessorkernen benötigt dieses Programm nur 30 % der Laufzeit der sequenziellen Variante.

Was nach dem Benutzen parallelisierter Bibliotheken als sequenzieller Programmcode verbleibt, sollte vornehmlich der Ablaufkontrolle und Benutzer-Interaktion dienen. Oftmals verbringt die Applikation aber viel Zeit in proprietären Komponenten. In diesem Fall muss man über Möglichkeiten der Parallelisierung nachdenken, wenn man Skalierung auf Mehrkern-Systemen sicherstellen möchte. Dazu eignen sich wie bei der Bibliotheksschicht aufgaben- oder datenparallele Verarbeitung.

Profiling hilft beim Parallelisieren

Bleibt die Frage, ob und wie man zeitkritische Komponenten im eigenen Applikationscode entdeckt, um Maßnahmen zu ihrer Parallelisierung ergreifen zu können. Von jeher helfen von der JVM generierte Profiling-Informationen bei der Analyse einer Java-Anwendung etwa mit HPROF (s. *iX*-Link). Deutlich mehr Komfort bieten die Profiling-Tools der verbreiteten IDEs. Sie erlauben nicht nur, die zeitkritischen Teile der Applikation zu finden, sondern in weiteren Ausbaustufen auch hakende Thread-Interaktionen (Kommunikation, Abhängigkeiten und so weiter) zu visualisieren. Beispiele dafür zeigt die Abbildung auf der vorigen Seite.

Leider ist der folgende Schritt des Refactorings des zeitkritischen Teils noch kaum zu automatisieren. Wenn passend, ist das aufgabenparallele Modell ein simpler, aber effektiver Ansatz, berechnungsintensive Algorithmen auf mehrere Prozessoren zu verteilen. Graph-Traversierungen, Raytracing und Video-Codecs mit komplizierterem Programmfluss (H.264) profitieren beispielsweise davon.

Fazit

Der Anteil an parallelem Code in Standard-Softwarekomponenten dürfte in Zukunft zunehmen. Das vergleichsweise einfache Beispiel des Rabin-Miller-Tests zeigt, dass Parallelverarbeitung naturgemäß komplex ist und deshalb nicht zum Repertoire jedes Informatikers gehören kann. Aus diesem Grund kommt Verfahren zum Verbergen dieser Komplexität eine besondere Bedeutung zu.

Java bietet bereits Mechanismen und Stellschrauben in der JVM sowie Abstraktionen zum Umgang mit aufgabenorientierter Parallelität. Bleibt zu hoffen, dass dieser Trend zur Parallelisierung sich in fundamentalen Frameworks fortsetzt, sodass Entwickler immer weniger parallelen Code selbst implementieren müssen. (ck)

NILS GRUSCHKA

ist Research Scientist bei den NEC Laboratories Europe und Spezialist für Sicherheit bei Web Service Systemen.

LUIGI LO IACONO

ist Senior Researcher bei den NEC Laboratories Europe und forscht an Sicherheitsfragen in diensteorientierten Systemen.

JÖRG WAGNER

ist Research Scientist bei den NEC Laboratories Europe und arbeitet an effizienten Schedulern für den Einsatz in eingebetteten Mehrkern-Systemen.

Literatur

[1] Sun Microsystems: Tuning Garbage Collection with the 5.0 Java Virtual Machine, Sun Developer Network, 2003

[2] Chris D. Johnson, Naresh Revanuru: JSR 237: Work Manager for Application Servers, Java Specification Requests, 2003

[3] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein; Introduction to Algorithms, MIT Press, Cambridge 2003

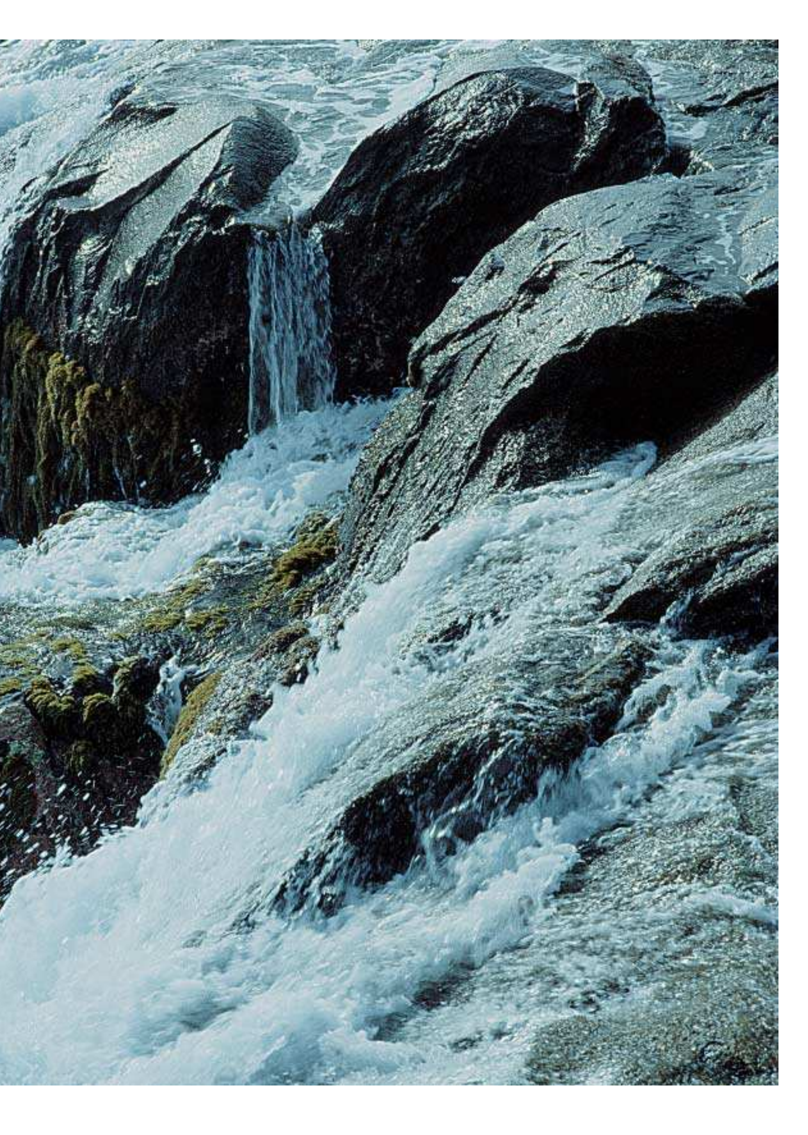
[4] Ivan Damgård, Peter Landrock, and Carl Pomerance, Average case error estimates for the strong probable prime test, Mathematics of Computation 61 (203), Seite 177-194, 1993







© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Aktuelle Techniken und Methoden fürs Media Streaming

Turbulente Strömungen

Horst Eidenberger

Videoportale und IPTV (IP Television) erobern das Internet. Doch das Übertragen zeitabhängiger Daten in Echtzeit – sogenanntes Streaming – stellt hohe Anforderungen an die Infrastruktur, die das paketvermittelte IP-Netz nicht immer erfüllen kann.

Nicht immer handelt es sich bei der Bereitstellung von Videos im Internet um echtes Streaming. Youtube etwa sendet die Daten per gewöhnlichem HTTP-Download. Progressives Herunterladen und Caching erlauben es, den Datenstrom wiederzugeben, bevor er vollständig vorliegt. Die Methode kommt häufig bei vergleichsweise kurzen Videoclips mit geringen Qualitätsanforderungen zum Einsatz.

Streaming in Echtzeit findet man eher beim Video On Demand (VOD), das ganze Kinofilme in hoher Qualität und bisweilen zu mehreren Empfängern gleichzeitig übertragen muss. Near Video On Demand (NVOD) ist ein ähnliches Verfahren, bei dem man Datenströme in fixen Zeitintervallen staffelt und wiederholt.

Unter einem Vodcast versteht man die Übertragung von Videos per Podcast. Dabei handelt es sich wiederum nicht um echtes Streaming, sondern um eine Download-Anwendung. Als Peercast schließlich bezeichnet man die – zurzeit experimentelle – Übertragung von Videodatenströmen in P2P-Netzen.

Datenströme in Pakete zerlegt

Ob VOD, NVOD oder Peercast – Streaming-Systeme bestehen stets aus den gleichen Komponenten (siehe Abbildung 1). Der Streaming-Server erhält seine Datenströme – aus der Konserve oder live erfasst von einer externen Quelle – in kodierter Form, eingeteilt in gleichartige Segmente (Chunks). Die überträgt er auf Anfrage zu den Streaming-Clients. Um die Last auf dem Server zu minimieren, legt man die Chunks häufig nachgefragter Datenströme in einem Cache ab. Der Sender muss lediglich Paket-Header mit Zeitstempeln, Reihungsinformationen und Qualitätsangaben für das verwendete Streaming-Protokoll hinzufügen.

Der Client entpackt die Daten und stellt den Mediendatenstrom wieder her. Erlaubt das Netz eine schnellere Datenübertragung, als man sie für Echtzeit braucht, kann er noch nicht benötigte Chunks wiederum in einem Cache ablegen.

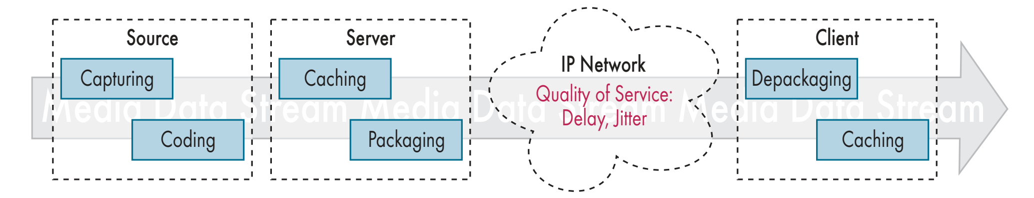
Taktgefühl ist unerlässlich

Schwierigkeiten ergeben sich hauptsächlich durch die Belastung des Servers und den Verlust beziehungsweise die Verzögerung von Paketen auf dem Übertragungsweg (Quality of Service, kurz QoS). Während man die Server-Last durch leistungsstarke Hardware und ausgefeilte Caching-Verfahren relativ einfach in den Griff bekommen kann, bleibt Quality of Service ein Dauerthema. Die Unwägbarkeiten der Paketvermittlung im IP-Netz (Flaschenhälse, Paketverluste et cetera) führen beim Client vor allem zu Delay und Jitter. Unter Delay versteht man die gleichförmige Verzögerung des Datenstroms; Jitter bezeichnet variable Zeitabstände zwischen Chunks. Während eine Verzögerung von bis zu einigen Sekunden für die meisten Menschen noch erträglich ist, führt Jitter zu unangenehmem Ruckeln von Bildteilen sowie teilweisen Bildausfällen und sollte daher vollständig vermieden werden. Bislang kann jedoch kein Verfahren zur Priorisierung des Routings von Mediendatenpaketen im Internet ausreichende QoS garantieren.

In den vergangenen Jahren haben die Leistungssteigerung der PC-Hardware und der Ausbau der Internet-Infrastruktur zur Verbreitung von Videodiensten und -anwendungen beigetragen. Im Sog dieser Entwicklung entstanden effizientere Kodierverfahren und Containerformate wie MPEG-4/H.264

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

und Flash Video (FLV). Trotz der Unterstützung moderner Protokolle auf den Internet-Routern bleibt QoS jedoch bis auf Weiteres außer Reichweite.



Lieferkette: Das IP-Netz verursacht beim Streamen die meisten Schwierigkeiten (Abb. 1).

Neue Codecs mit hoher Kompression

Insbesondere Videodatenströme sind zu breitbandig für eine unkomprimierte Übertragung. Der aktuelle Trend zu High-Definition-Medien mit hoher Auflösung und Framerate lässt die Anforderungen weiter steigen. Das schränkt die Zahl der verwendbaren Codecs ein. Heute kommen vor allem Sorensen (Apple Quicktime), Windows Media (Microsoft) und MPEG 4 zum Einsatz (siehe Abbildung 2). In dem aus vielen Teilen bestehenden MPEG-4-Standard sind insbesondere Part 2 (der „klassische“ MPEG-4-Video-Codec) und Part 10 (Advanced Video Coding, AVC) relevant. Letzterer ist lediglich ein Verweis auf den H.264-Codec der International Telecommunication Union (ITU).

H.264 repräsentiert mit skalierbarer Kodierung, multiplen Bewegungsvektoren und vielen anderen Features den aktuellen Stand der Video-Kompressionstechnik. Der Codec kommt unter anderem bei der Blu-Ray-Disc zum Einsatz. Sein designierter Nachfolger H.265 befindet sich noch in der Entwurfsphase und ist nicht vor 2012 zu erwarten. In der endgültigen Version soll er bis zu fünfzig Prozent schneller arbeiten als H.264.

Bei den Containerformaten gibt es hingegen wenig Neues. Die proprietären Klassiker Quicktime und Windows Media konkurrieren mit dem offenen MPEG-Format (nur für MPEG-Codecs) und Adobes relativ neuem Flash-Video-Format (FLV). Ursprünglich ausschließlich für die eigenen Codecs gedacht, unterstützt FLV seit Version 9 auch H.264 sowie den MPEG-4-Audiostandard Advanced Audio Coding (AAC). Allerdings kommt der Kernfunktion eines Containerformates, dem Multiplexen von Audio- und Videodatenströmen, im Streaming kaum Bedeutung zu: Die meisten Verfahren folgen dem Ansatz des Real-Time Transport Protocol (RTP), Audio und Video getrennt zu paketieren und zu übertragen.

Den offenen Streaming-Protokollen stehen ebenso viele proprietäre gegenüber. Auf der Anwendungsschicht etwa konkurriert das Real-Time Streaming Protocol (RTSP) mit Microsofts – mittlerweile offiziell aufgegebenem – Media Server



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Onlinequellen

RTP: A Transport Protocol For Real-Time Applications (RFC 3550)
tools.ietf.org/html/rfc3550

An Architecture for Differentiated Services (RFC 2475)
tools.ietf.org/html/rfc2475

International Telecommunication Union (ITU)
www.itu.int

Moving Picture Exprts Group (MPEG)
www.mpeg.org

Protocol MMS. RTSP ähnelt HTTP und bietet Steuerungsfunktionen zum Abspielen, Pausieren und Aufnehmen von Mediendatenströmen. Der Standard basiert auf einer älteren Version des Real-Time Transport Protocol.

Datenströme auf mehreren Wegen

RTP wurde 2003 überarbeitet und als RFC 3550 neu veröffentlicht (siehe Kasten „Onlinequellen“). Dabei hat sich die Funktionsweise allerdings kaum geändert. Nach wie vor trennt das Protokoll Daten nach Medientypen; für die heute relevanten Codecs kamen neue Payload-Typen hinzu. Für die Kontrolle der Übertragungsqualität zeichnet weiterhin das eingebettete Real-Time Transport Control Protocol (RTCP) verantwortlich. Es zählt unter anderem die verloren gegangenen und verspäteten Datenpakete. RTP ist hauptsächlich für den verbindungslosen Einsatz mit UDP gedacht, kann nun aber auch TCP-Verbindungen nutzen. Letzteres ist allerdings nur in leistungsfähigen Netzen sinnvoll, etwa im LAN. Ebenfalls neu hinzugekommen ist SRTP (Secure RTP), das die Protokolldaten nach dem Advanced Encryption Standard (AES) verschlüsselt.

Neben RTP entstanden in den letzten Jahren zahlreiche proprietäre Protokolle. Hervorzuheben ist das für die Übertragung von Flash-Daten entwickelte Real-Time Messaging Protocol (RTMP) von Adobe. Im Gegensatz zu RTP überträgt RTMP alle Mediendaten über einen einzigen TCP-Kanal. Dazu ist es notwendig, die Chunks der einzelnen Datenströme (Video, Audio) zu multiplexen. Da Chunks üblicherweise kurz sind, etwa 128 Byte, stattet RTMP die gemultiplexten Daten mit einem einzigen Paket-Header aus, der aufgrund der Verwendung von TCP nur wenig zusätzliche Informationen enthält und damit einen geringen Overhead verursacht. Außerdem kann RTMP Mediendaten in einem HTTP-Tunnel übertragen, etwa durch eine Firewall. Als Variante hat Adobe das Real-Time Media Flow Protocol (RTMFP) definiert. Es nutzt UDP und erlaubt daher schnelleren Transport, benötigt aber auch komplexere Paket-Header.

TCP gewinnt an Bedeutung

Auf der Transportschicht (Transport Layer) sieht sich das klassische Streaming-Protokoll UDP zunehmend der Konkurrenz von TCP ausgesetzt. In schnelleren Netzen überwiegen die Vorteile eines verbindungsorientierten Protokolls – gesicherte Übertragung und Fehlerkorrektur – die der ressourcensparenden verbindungslosen Übertragung. Neben den beiden Internet-Standards ist das Real Data Transport Protocol (RDT) von Real Networks zu nennen, das aber außerhalb des hauseigenen Helix-Streaming-Servers kaum zum Einsatz kommt.

In der Netzschicht regiert weiterhin IPv4. Erweiterungen wie das IP Multimedia Subsystem (IMS) bleiben auf mobile Anwendungen beschränkt. Daran dürfte sich auch mit IPv6 kaum etwas ändern. Solange keine streamingfreundlicheren Strukturen in das paketvermittelte Internet einziehen, sind die Möglichkeiten für Quality of Service jedoch stark eingeschränkt. Die vom Internet-Protokoll gebotene Best-Effort-Strategie ist für Mediendatenströme nicht akzeptabel.

Der ursprüngliche QoS-Ansatz – Reservierung eines Netzes vor der Datenübertragung (bekannt als Integrated Services, kurz IntServ) – ist zwar in kleinen Firmennetzwerken anwendbar. In der Weite des Internet aber nicht. Dort bleibt als Ausweg nur der IP-Multicast und das Hoffen auf Priorisierung der zeitkritischen Pakete durch die beteiligten Router. Dazu existiert mit den Differential Services (DiffServ) ein Klassifizierungs-Schema für Datenpakete, das von Best Effort (niedrigste Priorität) über Controlled Load (Echtzeitanforderung für Mediendaten) bis hin zu Reserved-Traffic-Klassen mit maximalen Verzögerungen von 100 beziehungsweise 10 Millisekunden reicht. Die Einhaltung der Prioritäten steht und fällt jedoch mit der eingesetzten Router-Hard- und -Software.

Fazit

Der Königsweg beim Streamen bleibt die Verwendung der offenen Protokolle RTSP, RTP/RTCP und UDP. Dabei sollten – falls möglich – auf der IP-Ebene Differential Services zur Sicherstellung der Quality of Service zum Einsatz kommen. Zur Optimierung der Videoqualität empfiehlt sich das Medienformat MPEG-4 Part 10 (H.264). Grundlegend neue Konzepte wie Peer-Streaming sind noch weit von der täglichen Anwendung entfernt. Beim Peercasting ist aufgrund der zu erwartenden rechtlichen Schwierigkeiten zudem fraglich, ob es sich jemals auf breiter Fläche durchsetzen kann. (mr)

Raw Media Stream
Content Types | MP4/H.264 | Sorensen | WMV
Container Types | MPEG | FLV | WMF
Media Coding
Application and Session Layers | RTSP | HTTP | MMS
RTP/SRTP | RTMFP | RTMP
Transport Layer | UDP | RDT | TCP
Network Layer | IP + IP Multicast
Network Stack
Data Packets
Encode
Decode

Echte Streaming-Protokolle wie RTSP und RTP konkurrieren mit anwendungsfremden wie HTTP und TCP. Offene Standards sind hellblau hinterlegt, proprietäre dunkelblau (Abb. 2).

DR. HORST EIDENBERGER

ist außerordentlicher Professor an der TU Wien und zertifizierter Gutachter am Handelsgericht Wien.

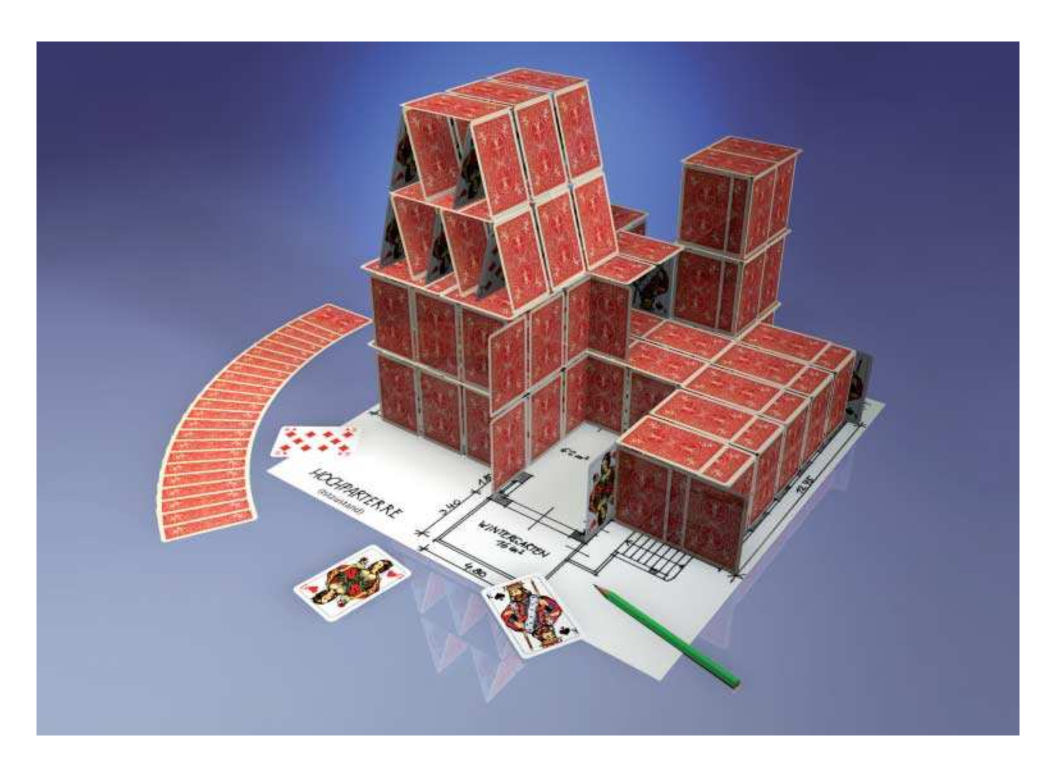




© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Systematisches Softwaredesign in der Nussschale

Bubbles don't crash

Michael Stal

Der Erfolg eines Softwareprojekts steht und fällt mit der Architektur eines Systems. Nicht immer führen anfängliche schnelle Erfolge zu einer stabilen Software. Mit welchen Herausforderungen sich ein Softwarearchitekt initial und im Laufe des Projekts konfrontiert sieht, lässt sich am Beispiel des fiktiven Bob nachvollziehen.

Nach seiner Umschulung zum Softwareentwickler steht Bob, der Baumeister, vor der ersten großen Herausforderung. Zusammen mit anderen Leidensgenossen soll er die Softwarearchitektur für einen Webshop erstellen. Was er zunächst für ein lächerlich einfaches Projekt hielt, erweist sich auf dem zweiten Blick als ganz und gar nicht trivial. Vor ihm steht bedrohlich ein weißes, bislang gähnend leeres Flip-Chart. Es scheint sehnsüchtig darauf zu warten, dass Bob es mit architektonischen Entwürfen füllt.

Bob sieht sich mit diversen Herausforderungen konfrontiert. Er muss überlegen, welches der erste Schritt im Architekturentwurf ist, und wie er anschließend systematisch das Softwaresystem erstellt. Außerdem muss er sich klarmachen, welche Informationen und Voraussetzungen zu gewährleisten sind. Dieser Artikel konzentriert sich ganz auf diese architektonische Brille. Details wie der Entwicklungsprozess oder die Rolle des Architekten sind nicht Gegenstand der Betrachtungen.

Offensichtlich benötigt der Softwarearchitekt Bob am Anfang eine Liste von hinreichend detaillierten Anforderungen, allesamt mit eindeutigen Prioritäten versehen. Wie vollständig eine solche Liste sein muss, daran scheiden sich bisweilen die Geister. Dass schon zu Beginn alle Anforderungen vorliegen, entspricht zwar dem Ideal, dürfte aber bei komplexeren Projekten dem Finden des heiligen Grals gleichkommen. Übrigens mit ein Grund dafür, warum Wasserfallmodelle sich oft als Sackgasse erwiesen haben. Einer „Mission Impossible“ gleicht das andere Extrem, das mit keinen oder wenigen Anforderungen auskommen will. Es führt letztendlich zu übergenerischen Softwarearchitekturen, die es keinem recht machen können, weil sie es allen recht machen wollen. Die Wahrheit liegt also irgendwo in der Mitte.

Conditio sine qua non

Je mehr architektonisch signifikante Anforderungen bekannt sind, desto stabiler das architektonische Fundament. Damit sich der Architekt in Konfliktsituationen für das richtige Vorgehen entscheiden kann – ähnlich der Rechts-vor-links-Regel im Straßenverkehr – sollten diese Anforderungen eindeutige Prioritäten besitzen. Meistens stammen die Anforderungen nicht von den Softwareentwicklern, sondern von Anforderungsingenieuren, Produktmanagern oder Kunden. Daher kommt der Kommunikation mit dem genannten Personenkreis essenzielle Bedeutung zu, was bedeutet, dass sich der Alltag des Softwarearchitekten nicht auf technische Aspekte beschränkt. Nicht immer sind die Anforderungen verständlich, detailliert und widerspruchsfrei formuliert oder haben eindeutige Prioritäten. Hier heißt es oft, intensiv nachzubohren und bisweilen Überzeugungsarbeit zu leisten.

Damit Softwarearchitekten in einem konkreten Projekt die Ziele ihrer Organisation oder ihrer Kunden unterstützen können, benötigen sie grundlegendes Wissen über geschäftliche Aspekte. Je nach Kontext kann es zum Beispiel in einem Fall sinnvoll sein, wichtige Teile des Systems mithilfe von Offshoring-Maßnahmen zu entwickeln und die Architektur entsprechend zu planen, während sich dieses Vorgehen in einem anderen Fall vollkommen verbietet. Zudem lässt sich manche geschäftliche Zielvorgabe überhaupt nicht umsetzen, zumindest nicht mit vernünftigem Aufwand. Basiswissen über grundlegende

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Instrumente und nichttechnische Softwarearchitekturaspekte erweist sich daher in diesem Zusammenhang als unbedingt erforderlich.

Zu guter Letzt müssen Softwarearchitekten sowohl die fachliche Problemdomäne als auch die technischen Lösungsdomänen verstehen. Fehlt ihnen die geistige Durchdringung der Fachdomäne, bleibt die Problemstellung im Dunkeln. Haben sie nur unzureichende Kenntnisse der Lösungsdomänen, können sie keine technisch fundierten Ergebnisse erzielen. Wie sagte Bertrand Meyer einst so schön: „Bubbles don't crash."

Softwarearchitektur – was ist das?

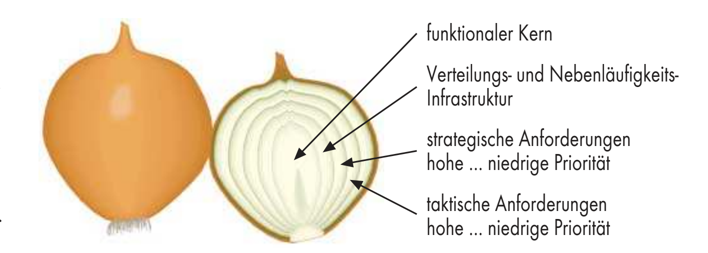
Bob denkt an seine Umschulung zurück. Für den Begriff „Softwarearchitektur" gibt es mindestens ebenso viele Definitionen, wie die Menschheit Gottesbeweise hervorgebracht hat. Zum Glück besitzen die diversen Definitionen mehr Gemeinsamkeiten als Unterschiede. Softwarearchitektur beschreibt demnach die Komposition eines Softwaresystems aus Subsystemen, deren Beziehungen zueinander sowie die Grundprinzipien, mit deren Hilfe die Architekten die Anwendung erstellen.

Hinzuzufügen ist an dieser Stelle, dass der Blick auf eine Softwarearchitektur immer aus verschiedenen Perspektiven (Viewpoints) erfolgen muss. Demzufolge geben die verbreiteten Diagramme, die lediglich eine Menge von Rechtecken über eine Menge von Linien verbinden, nicht wirklich die Softwarearchitektur wieder. Es bedarf stattdessen weiterer Beschreibungen des Systems, etwa der Interaktionen zwischen den Komponenten oder der Systemzustände. Und da bloße Syntax nichts anderes repräsentiert als Kreidehaufen, gehört zur Softwarearchitektur neben dem „Was" immer auch das „Warum", also das Rationale für alle architektonischen Entscheidungen. Mit einer Sammlung von UML-Diagrammen ist es demnach nicht getan.

Aber was hat es mit den ominösen Grundprinzipien auf sich, die sich in der obigen Definition verstecken, fragt sich Bob. Dass viele Köche den Brei verderben, gilt nicht zuletzt auch für die Softwareentwicklung. Wenn ein Entwickler zur Fehlerbehandlung Ausnahmen wirft, während ein anderer Fehlerwerte zurückgibt und ein dritter Informationen in ein Logbuch schreibt, befinden sich unvermittelt drei Varianten der Fehlerbehandlung im System. Treten zudem im selben Architekturentwurf verschiedene Softwaremuster zur Lösung ähnlicher Problemstellungen auf, leidet die daraus resultierende Softwarearchitektur an Qualitätsmängeln, beispielsweise an schlechter Verständlichkeit und geringer Symmetrie. Daher sollten Bob und seine Koarchitekten schon zu Beginn des Projekts dafür sorgen, dass sie einheitliche Entwurfskonventionen und -regeln einführen. Mit der Erstellung von Dokumenten ist es allerdings nicht getan. Vielmehr müssen sie die Einhaltung aller Vorgaben und Konventionen auch regelmäßig kontrollieren.

Anforderungen ermitteln
Feedback-Schleife
Kreation der Architekturbasis
Evaluieren und Verfeinern der Architektur
Refaktorieren der Architektur
nein
fertig ?
ja
ausführbare Architektur

Ein systematischer Prozess für den Architekturentwurf ist inkrementell und ermittelt zu Beginn alle architektonisch relevanten Anforderungen (Abb. 1).



Das Zwiebelmodell veranschaulicht die richtige Reihenfolge beim Entwurf: Zuerst die fachlichen Aspekte, dann die nichtfachlichen, jeweils mit absteigender Tendenz (Abb. 2).

Prioritäten des Zwiebelmodells

Das Prinzip der systematischen Architekturerstellung lässt sich am besten anhand einer Zwiebel illustrieren, was nicht nur daran liegt, dass die architektonischen Anstrengungen Bob bisweilen Tränen in die Augen treiben. Zu Beginn des Entwurfs und damit im Kern des Zwiebelmodells steht das fachliche Objektmodell. Bob überlegt, aus welchen fachlichen Entitäten sich ein Webshop zusammensetzt. Da wären zum Beispiel der Produktkatalog, der Warenkorb, das Zahlungssubsystem, die Kundendatenbank, das Logistik- und das Bestellsystem. Natürlich fristen diese Objekte kein Inseldasein, sondern haben Beziehungen zueinander. Ein Warenkorb muss mit dem Produktkatalog interagieren, ebenso mit dem Bezahlsystem.

Fragt sich, wie Bob diese Beziehungen eruieren kann. Im Idealfall existiert für die Problemstellung bereits eine allgemein bewährte Referenzarchitektur für Webshops, derer er sich bedienen kann. Leider gibt es solche Vorlagen nur für wenige Anwendungsdomänen. Daher greift der Softwarearchitekt im Normalfall zu Anwendungsszenarien – zu Neudeutsch Use Cases –, um die Erwartungen an das Zielsystem aus der Vogelperspektive zu beschreiben, sowie zu einem Kontextdiagramm, um zu definieren, welche Entitäten sich im System und welche sich außerhalb befinden.

Für den Webshop ermittelt Bob dabei eine Reihe von Anwendungsfällen, etwa „Im Produktkatalog suchen", „Produkt zu Warenkorb hinzufügen" oder „Warenkorb bestellen". Da der Kunde das existierende SAP-Warenwirtschaftssystem zur Verwaltung von Bestellungen verwenden möchte, befindet sich die SAP-Schnittstelle im Kontextdiagramm außerhalb des Webshops, ebenso wie das Logistiksystem oder die notwendigen Schnittstellen zu Banken und Kreditkartenfirmen. Aus den Anwendungsfällen und dem Domänenwissen ergibt sich nun inkrementell ein grobgranulares fachliches Objektmodell.

iX-TRACT

- Softwarearchitekten sind dafür verantwortlich, alle Fäden in der Hand zu halten. Sie benötigen hierfür fachliches Wissen, Domänenkenntnisse und soziale Fähigkeiten.
- Anforderungen fließen systematisch in den Systementwurf ein, beginnend mit einem funktionalen Kern, über strategisches bis zum taktischen Design.
- Das Nutzen von Softwaremustern sorgt für mehr Produktivität, da es hilft, unnötige Kosten zu vermeiden.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Für den Übergang der von Use Cases propagierten Black-Box- zu einer White-Box-Sicht mit detaillierten Abläufen existiert leider kein Automatismus. Dass es für Bobs Webshop einen Anwendungsfall „Warenkorb bestellen“ gibt, ist eine Sache. Wie die internen Komponenten zur Realisierung dieses Anwendungsfalles zusammen spielen müssen, eine ganz andere. Die Softwarearchitekten stützen sich auf ihre Domänenkenntnisse, um aus Use Cases etwa Sequenzdiagramme abzuleiten.

Muster erleichtern das Leben

Für die generelle Strukturierung der Gesamtarchitektur bieten sich die sogenannten architektonischen Muster an, zu denen beispielsweise Layers, MVC (Model-View-Controller) oder Pipes-and-Filters gehören. Dass sich eine webbasierte Geschäftsanwendung wie Bobs Webshop gut mittels eines Mehrschichtenmodells entwerfen lässt, dürfte inzwischen zum Allgemeinwissen gehören. Ebenso, dass Techniken wie Ruby on Rails, JSF, Struts oder ASP.Net ein Anwenden des MVC-Musters forcieren. Überhaupt empfiehlt sich das Nutzen von Softwaremustern für alle Granularitätsebenen des Designs, wollen Entwickler nicht ständig das Rad neu erfinden. Was wieder auf die Grundprinzipien der Architekturerstellung zurückführt. Bobs Bibliothek enthält daher die entsprechende Standardliteratur in Griffweite.

Erfahrungsgemäß scheitern viele Softwareentwicklungsprojekte weniger an den funktionalen Aspekten. Der Knackpunkt besteht stattdessen oft in der Umsetzung nichtfunktionaler Qualitäten. Die übliche Wunschliste operationaler Eigenschaften wie 99,999 % Verfügbarkeit oder Skalierbarkeit bis 100 000 Kunden lässt sich ebenso wenig en passant realisieren wie entwicklungstechnische Eigenschaften à la leichte Änderbarkeit oder Administrierbarkeit. Gerade die operationalen Eigenschaften eines Softwaresystems beeinflussen dessen Architektur als Ganzes, während entwicklungstechnische Eigenschaften oft nur lokalen Einfluss auf eines oder wenige Subsysteme haben. Trotzdem stürzen sich viele Softwarearchitekten oft zuerst auf Letztere. Ein Strategy-Muster hier und da und vielleicht noch ganz woanders zur vermeintlich besseren Änderbarkeit – schon krankt die gesamte Softwarearchitektur am Strategy-Syndrom und mutiert zu einem schwer beherrschbaren, übergenerischen Softwaresystem.

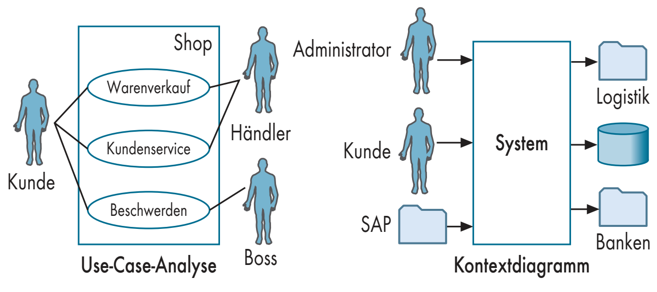
Drei Ebenen sind genug

Ein systematisches Vorgehen sieht anders aus. Grundsätzlich lassen sich drei Ebenen beziehungsweise Phasen in der besagten Zwiebel unterscheiden, sobald Bob das fachliche Objektmodell seines Webshops mit nichtfachlichen Aspekten schmücken will.

Phase I – Verteilung und Parallelität: Zu Beginn sind die meisten Softwaresysteme heutzutage als nebenläufige und verteilte Systeme konzipiert. Ein Webshop läuft in der Regel auf einem vom Kunden separierten Server und benutzt Parallelitätskonzepte, um Skalierbarkeits- und Performanceanforderungen zu erfüllen. Dies impliziert, dass der vorliegende funktionale Kern in eine verteilte, nebenläufige Infrastruktur einzubetten ist. Für die Trennung der Präsentationsschicht von den Geschäftskomponenten sowie deren Separation von EIS-Systemen (Enterprise Information Systems) wie Datenbanken oder ERP-Anwendungen bieten sich broker- und komponentenbasierte Softwarearchitekturen an. Und auch hier finden sich wieder die Softwaremuster für verteilte und nebenläufige Systeme. Genau genommen entwirft der Softwarearchitekt eine passende Infrastruktur für Verteilung und Parallelität, in die er anschließend das bereits vorhandene fachliche Objektmodell integriert. Das resultierende Architekturmodell dient dann als Basis für die weiteren Phasen.

Phase II – strategisches Design: Nun erfolgt der strategische Entwurf. Für alle operationalen Eigenschaften erstellen Bob und seine Freunde ebenfalls passende Infrastrukturen. Dabei orientieren sie sich hinsichtlich der Reihenfolge an den vorgegebenen Prioritäten. Würde also Sicherheit die wichtigste operationale Eigenschaft darstellen, müssten sie zunächst gemäß der vorliegenden Anforderungsbeschreibung eine Sicherheitsinfrastruktur konstruieren, die Subsysteme beziehungsweise Komponenten wie Firewalls, Sicherheitsprotokolle oder Authentisierungsserver beinhaltet. Diese Infrastruktur integrieren sie in die bisherige Architektur. Danach folgen die weiteren operationalen Anforderungen mit absteigender Priorität. Je weiter innen im Zwiebelmodell eine solche Eigenschaft liegt, desto mehr Einfluss hat sie naturgemäß auf die gesamte Softwarearchitektur. Ein Web-Shop, der in erster Linie sicher und nur in zweiter Linie verfügbar sein soll, besitzt folgerichtig eine andere Softwarearchitektur als einer, der primär mit Verfügbarkeit und sekundär mit Sicherheit glänzen will. Mindestens für die wichtigsten operationalen Eigenschaften sollten Entwicklungsprojekte eigene Experten oder sogar ganze Teams spendieren, die sich hauptsächlich um genau diese nichtfachlichen Aspekte kümmern. Grundsätzlich ließen sich natürlich auch Verteilung und Nebenläufigkeit als operationale Eigenschaften charakterisieren. Da diese Aspekte aber normalerweise über andere operationale Eigenschaften dominieren, ist es sinnvoll, zwischen den beschriebenen Phasen I und II zu unterscheiden.

Phase III – taktisches Design: Es lässt sich trefflich darüber streiten, wo architektonisches Design endet und Softwaredesign beginnt. Oft betrachten Experten Architektur- und Softwaredesign als Synonyme. Im taktischen Entwurf konzentrieren sich Architekten auf die entwicklungstechnischen Eigenschaften. Dazu zählen unter anderem Wartbarkeit, Erweiterbarkeit, Änderbarkeit und Testbarkeit. Es handelt sich also um Anforderungen, die weniger das Laufzeitverhalten der Anwendung als viel mehr deren Entwicklung oder Evolution betreffen. Nicht immer leuchtet den Projektbeteiligten allerdings ein, warum so wichtige Eigenschaften wie Änderbarkeit erst am Schluss einfließen. Gerade derlei Qualitäten sollten sich aber in einem stabilen Fundament begründen statt im Chaos. Bei Flexibilitätsanforderungen bietet sich die Commonality/Variability-Analyse als adäquates Instrument an. Diese stellt fest, welche Bestandteile der Anwendung



Use Cases repräsentieren als Black-Box-Sicht alle Erwartungen an das System seitens der Benutzer. Ein Kontextdiagramm klärt, was innerhalb und außerhalb des Systems sein soll (Abb. 3).

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

invariant und welche variabel sein sollen. Erstere beeinflussen die Softwarearchitektur bereits in früheren Entwurfsphasen, während Letztere im taktischen Design zum Tragen kommen. Zwei Beispiele mögen das illustrieren:

Bob hat bereits im funktionalen Entwurf berücksichtigt, dass jeder Web-Shop über ein Bezahlsystem verfügen muss. Andererseits soll der Webshop für verschiedene Kunden zum Einsatz kommen, deren Wünsche bezüglich der Zahlungsoptionen variieren können. Während einige Online-Shops Zahlung per Rechnung offerieren, beschränken sich andere auf Einzugsermächtigung oder Vorkasse. Die Art der Zahlung stellt somit eine Variabilität dar, während die Notwendigkeit des Bestellsystems selbst eine Invariante repräsentiert.

Skalierbarkeit ihrer Web-Shops wünschen natürlich alle Kunden. Deren potenzielles Ausmaß ist allerdings direkt proportional zu ihren finanziellen Möglichkeiten. So könnte Bob neben Web- auch Applikationsserver und Datenbanken replizieren und über Komponenten für Lastverteilung ansteuern. Oder er beschränkt sich auf die kostengünstigere Variante, die lediglich eine Replikation der Webserver vorsieht und alle Softwareserveranwendungen parallel vorhält. Letztere Variante sieht Bob deshalb für alle Kundenszenarien vor, betrachtet das Replizieren von Applikationsservern und Datenbankservern aber als optional.

Die Reihenfolge beim Einbringen taktischer Eigenschaften bestimmt Bob erneut anhand eindeutiger Prioritäten. Am Ende seiner Bemühungen steht er vor der vollendeten Zwiebel beziehungsweise vor einer stabilen Basisarchitektur, die als Fundament für die nachfolgenden Verfeinerungsschritte dient. Auf die Implementierungsphase selbst kann dieser Artikel nicht weiter eingehen.

Der Teufel steckt im Detail

Irgendwann während seiner architektonischen Schwerstarbeit stellt sich Bob die philosophische Frage, wie detailliert die Basisarchitektur für den Web-Shop überhaupt sein muss. Wie weit sollte der Softwarearchitekt also gehen und wann beginnt die eigentliche Implementierungsphase? In einigen Projekten soll die Entwurfsphase angeblich schon unüberschaubare Ausmaße angenommen haben und so mancher Kunde vor Beendigung des Projektes dahingeschieden sein. Eine wissenschaftlich fundierte Antwort gibt es hierfür leider nicht, wohl aber eine Daumenregel. Und weil Bilder oft mehr sagen als tausend Worte, möge das Pyramidenmodell (Abbildung 4) der Veranschaulichung dienen. Die Architektur eines Softwaresystems umfasst demnach maximal drei Ebenen: das System als Ganzes, die grundlegenden Subsysteme und ihre Beziehungen sowie die Komponenten, aus denen sich wiederum die Subsysteme konstituieren.

Die Abbildung der mehrdeutigen Begriffe Subsysteme oder Komponenten auf reale Entitäten hängt vom Problemkontext ab. In einem serviceorientierten Umfeld könnten die Subsysteme zum Beispiel Dienste darstellen, die sich ihrerseits aus Komponenten zusammensetzen. Für Kleinstsysteme könnten Subsysteme zu Komponenten und Komponenten zu Klassen mutieren.

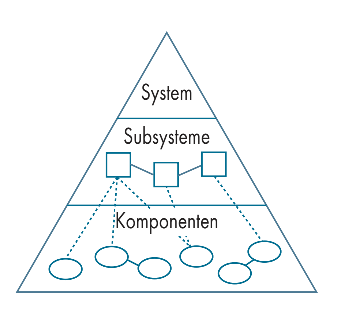
Onlinequellen	
Grady Booch; Handbook of Software Architecture	www.booch.com/architecture/index.jsp
Carnegie-Mellon University	www.sei.cmu.edu/architecture/
Michael Stals Architekturblog	stal.blogspot.com

Bekanntlich beginnen die wenigsten Softwareprojekte auf der grünen Wiese. Da wünschen Auftraggeber die Nutzung eines speziellen Datenbanksystems für ihren Web-Shop oder fordern die optimale Nutzung eines bestimmten Betriebssystems. Ein Extrem stellen in diesem Zusammenhang eingebettete und Echtzeitsysteme dar, weil sie stringente Vorgaben hinsichtlich Laufzeitverhalten und Ressourcennutzung implizieren. Hier stellt sich die Frage, ob solche Aspekte überhaupt ins bisherige Bild passen oder derartige Systeme einen gänzlich anderen Prozess benötigen. Zum Glück lassen sich die beschriebenen Prinzipien auch auf diese Problemkontexte anwenden, sofern die Softwarearchitekten die genannten stringenten Vorgaben als Anforderungen höchster Priorität betrachten. Im Zwiebelmodell müsste Bob also von Anfang an Vorgaben wie die Begrenzung auf 512 KByte Hauptspeicher berücksichtigen.

Fazit

Bob ist überglücklich, nachdem er sein erstes Projekt erfolgreich zu Ende geführt hat. Er hat gelernt, dass erfolgreiche Softwarearchitekturen sich nur in einem systematischen und inkrementellen Prozess realisieren lassen, wie dies auch bei allen anderen Ingenieursdisziplinen der Fall ist. Ad-hoc getriebene Ansätze hingegen erwecken zwar mitunter anfangs die Illusion eines rasanten Fortschritts, scheitern dann aber an der Komplexität der Problemstellung, die den Beteiligten schon bald hoffnungslos über den Kopf wächst.

Natürlich muss das Verhältnis von Planung und Umsetzung in einem vernünftigen Verhältnis stehen. Man kann sich auch zu Tode planen, wie einige Großprojekte aus jüngster Zeit beweisen. Der Architekt sollte über ein ausreichendes Fundament an Erfahrung und Wissen verfügen, das sich



Um sich nicht in Details zu verlieren, schlägt das Pyramidenmodell einen dreistufigen Ansatz vor (Abb. 4).

von der Domänenexpertise über Technik- und Methodenkenntnisse bis zu sozialen Fähigkeiten erstreckt.

Und zu guter Letzt sollten Softwarearchitekten nicht nach Innovation, sondern nach Lösungen streben. Der erste Trägheitssatz der Softwarearchitektur postuliert nicht umsonst die ausgiebige Nutzung von Softwaremustern und anderen bewährten Praktiken, um die Produktivität und Effektivität zu steigern. Und ganz nebenbei verbessert sich dadurch Bobs Work-Life-Balance, aber das ist eine andere Geschichte. (ka)

DR. MICHAEL STAL

ist bei der Corporate Technology der Siemens AG als Principal Engineer tätig und beschäftigt sich mit verteilten Systemen und Softwarearchitekturen. Er ist unter anderem Koautor der Buchserie Pattern-Oriented Software Architecture.

Literatur

[1] Paul Clements, Linda Northrop; Software Product Lines; Practices and Patterns; Addison-Wesley, 2002

[2] Alistair Cockburn; Writing Effective Use Cases; Addison-Wesley, 2000

[3] Paul Dyson, Andrew Longshaw; Architecting Enterprise Solutions; Patterns for High-Capability Internet-Based Systems; Wiley, 2004





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Zentrales Sicherheitsinformationssystem FreeIPA

Identitäts-Voodoo

Thorsten Scherf



Zentrale Lösungen zur Benutzerverwaltung mit Single-Sign-On-Eigenschaften existieren auch im Open-Source-Umfeld in großer Zahl. Jedoch sind die meisten recht umständlich zu implementieren und zu administrieren oder sie bieten nicht den gewünschten Funktionsumfang. Abhilfe verspricht das freie Sicherheitsinformationssystem FreeIPA.

Klassischerweise setzen sich die Anforderungen an aktuelle IT-Landschaften aus drei Punkten zusammen: Compliance/Kompatibilität, Risikoreduzierung sowie Effektivität. Ziel einer IT-Compliance ist nicht nur die Einhaltung nationaler (Telekommunikationsgesetz, Bundesdatenschutzgesetz) sondern gegebenenfalls auch internationaler Regelungen (Basel-II, Sarbanes-Oxley). Problem- und Gefahrenpotenziale sind zu erkennen und durch geeignete Maßnahmen dauerhaft zu vermeiden beziehungsweise zu beseitigen. In Deutschland gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI, siehe „Onlinequellen“ [a]) seine umfangreichen Grundschutz-Kataloge heraus, die potenzielle Risiken mit konkreten Handlungsanweisungen kombinieren. Einige grundlegende Details liefert der Kasten „Grundschutz-Forderungen“.

Natürlich existieren für die dort genannten Anforderungen schon viele Ansätze, beispielsweise in Form eines LDAP-Servers für die Benutzerverwaltung. Zur sicheren Verwaltung von Passwörter existiert seit langer Zeit das Kerberos-Protokoll, der Audit-Daemon [1] kann sämtliche Benutzer- und Prozessaktivitäten nachverfolgen und schließlich lässt sich mit SELinux eine extrem fein granulierte Sicherheits-Policy auf Basis der Mandatory Access Control einrichten. Der Nachteil hier besteht darin, dass alle genannten Lösungen Stand-alone-Produkte sind und sich nur mit großem administrativen Aufwand an zentraler Stelle miteinander kombinieren lassen. So lassen sich beispielsweise die Audit-Logs mehrerer Maschinen nicht zentral verwalten. Auch das Verteilen einmal erzeugter SELinux-Policy-Module auf mehrere Maschinen funktioniert ohne selbstgebaute Skripte bisher nicht. Zwar existiert eine Vielzahl von proprietären Lösungen, jedoch sind diese meist recht teuer und unflexibel, wenn man sie mit bestehenden Produkten aus der Open-Source-Welt vergleicht. Erschwerend kommt oftmals hinzu, dass die Interoperabilität mit Linux-Systemen nicht gerade die Beste ist.

Eine weitere Alternative besteht im Einsatz von Microsofts Active Directory (AD). Hierbei handelt es sich um einen erprobten Directory-Server auf LDAP/Kerberos-Basis, den viele IT-Abteilungen schon einsetzen. Sieht man von der fehlenden nativen Schnittstelle für die Authentifizierung von Linux-Benutzern einmal ab, spricht im Prinzip nichts dagegen, diesen Server zur Authentifizierung

iX-TRACT

- Für Single Sign-On existieren unter Linux viele Ansätze, die sich meist durch komplizierte Verwaltung oder unvollständigen Funktionsumfang für einen praktischen Einsatz disqualifizieren.
- FreeIPA will die Verwaltung von Identitäten, Policies und Audit-Protokollen koordinieren und zusammenführen.
- Dazu vereint das freie Projekt in klassischer Unix-Manier bereits vorhandene Ansätze unter einem leicht zu bedienenden Web-Frontend nebst einigen Kommandozeilenwerkzeugen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

von sowohl Linux- als auch Windows-Benutzern einzusetzen. Das in Ausgabe 10/08 begonnene *iX*-Tutorial [2, 3] befasst sich ausführlich mit dieser Fragestellung.

Varianten für Linux-Umgebungen

Für das Andocken von Linux-Umgebungen an AD existiert das ebenfalls erprobte Samba oder beispielsweise Likewise [b]. Ein großer Nachteil hier besteht darin, dass im AD kein Policy- oder Audit-Management für Linux-Systeme existiert. Hierfür müsste man wieder auf andere Programme zurückgreifen, was den Produkt-Dschungel wieder vergrößern würde – und genau dies möchte man ja vermeiden. Zusätzlich ließe sich noch darüber diskutieren, ob man sicherheitsrelevante Daten beziehungsweise Informationen wirklich in die Hand eines Anbieters geben möchte, wenn man die Funktionen des eingesetzten Programms überhaupt nicht nachvollziehen kann.

Genau in diese Kerbe schlägt das Projekt FreeIPA [c], eine kommerzielle Variante gibt es als Red Hats IPA [d]. Hiermit lässt sich sowohl eine zentrale Verwaltung von Identitäten (I), Policies (P) wie auch der Audit-Logs (A) realisieren. In guter alter Unix-Manier erfindet das Projekt das Rad nicht immer wieder neu, sondern greift stattdessen auf existierende Ansätze zurück und vereint diese unter einem leicht zu bedienenden Web-Frontend oder wahlweise einer Handvoll Kommandozeilen-Tools (siehe Abb. 1).

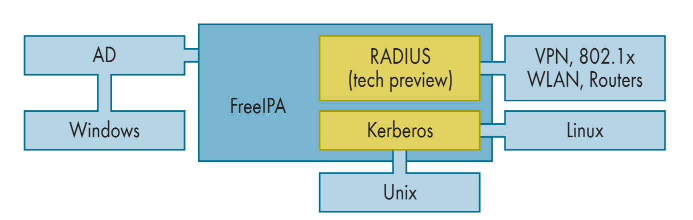
FreeIPA ist ein noch recht junges Open-Source-Projekt. In der aktuellen Version 1.1 liegt der Fokus auf dem Identity-Management, in der für Anfang 2009 erwarteten Version 2.0 sollen die Policy- und Audit-Komponenten folgen. Durch ein modulares Konzept lassen sich dem Core-System die verschiedensten Komponenten hinzufügen. So soll in Zukunft beispielsweise Dogtag [e], die Open-Source-Variante von Red Hats Zertifikatssystem, die Verwaltung der X.509-Zertifikate übernehmen, FreeRADIUS für RAS-Benutzer und der bekannte *audit*-Daemon für die zentrale Speicherung von Audit-Informationen zuständig sein. Den Zugriff auf die einzelnen Komponenten der IPA-Version 1 zeigt Bild 2.

Wie die Grafik schön zeigt, lassen sich mit FreeIPA auch die Konten eines vorhandenen AD mit einem IPA-Server synchronisieren. Somit kann man Linux- und Unix-Benutzern einfach eine native Schnittstelle für die Authentifizierung mit AD-Konten bieten. Ein weiterer Vorteil im Vergleich zur direkten Anmeldung an einem AD-Server.

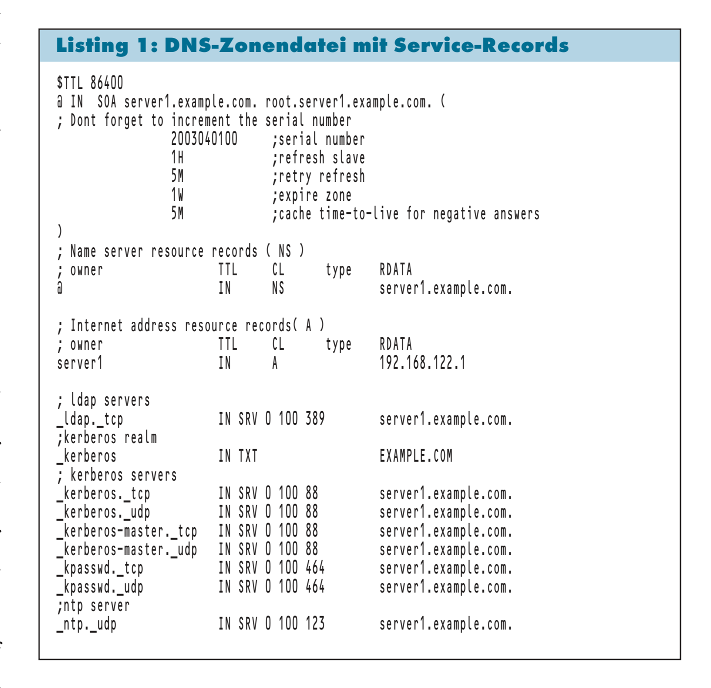
Fedora Server Installation

Eine einfache Installation des IPA-Servers war eine grundlegende Voraussetzung bei der Entwicklung und so ist es nun tatsächlich möglich, das komplette Setup innerhalb weniger Minuten zu bewerkstelligen. Da FreeIPA in den Repositories von Fedora 8 und 9 enthalten ist, reicht der Aufruf *yum install -y ipa-server*, um alle notwendigen Pakete einzuspielen. Vor dem Aufruf des Installationsskripts sollte man sicherstellen, dass die Namensauflösung für den IPA-Server reibungslos funktioniert. Steht für die Domäne noch kein DNS-Server zur Verfügung, so beschreibt Shannon Hughes in einem Online-Artikel [f] eine einfache Bind-Installation. Ein DNS-Server zur Namensauflösung ist auch für die IPA-Clients hilfreich, da diese dann über einen Service-Discovery ihre zuständigen Server finden und somit nicht manuell zu konfigurieren sind. Der Aufruf *ipa-server-install* startet die Setup-Routine und erzeugt unter anderem eine DNS-Zonendatei mit den passenden Service-Einträgen

Zum Verwalten des IPA-Servers stehen sowohl Kommandozeilen-Tools als auch ein Web-Frontend zur Verfügung (Abb. 1).



Auf den IPA-Server können die Clients auf unterschiedliche Wege zugreifen (Abb. 2).



Listing 1: DNS-Zonendatei mit Service-Records

```
$TTL 86400
@ IN  SOA server1.example.com. root.server1.example.com. (
; Dont forget to increment the serial number
                2003040100      ;serial number
                1H              ;refresh slave
                5M              ;retry refresh
                1W              ;expire zone
                5M              ;cache time-to-live for negative answers
)
; Name server resource records ( NS )
; owner                 TTL     CL      type    RDATA
@                       IN      NS              server1.example.com.

; Internet address resource records( A )
; owner                 TTL     CL      type    RDATA
server1                 IN      A               192.168.122.1

; ldap servers
_ldap._tcp              IN SRV 0 100 389        server1.example.com.
;kerberos realm
_kerberos               IN TXT                  EXAMPLE.COM
; kerberos servers
_kerberos._tcp          IN SRV 0 100 88         server1.example.com.
_kerberos._udp          IN SRV 0 100 88         server1.example.com.
_kerberos-master._tcp   IN SRV 0 100 88         server1.example.com.
_kerberos-master._udp   IN SRV 0 100 88         server1.example.com.
_kpasswd._tcp           IN SRV 0 100 464        server1.example.com.
_kpasswd._udp           IN SRV 0 100 464        server1.example.com.
;ntp server
_ntp._udp               IN SRV 0 100 123        server1.example.com.
```

(SRV records). Darüber können Clients alle notwendigen Informationen wie LDAP- und Kerberos-Server-IP, Kerberos-Realm et cetera direkt aus dem DNS beziehen, eine umständliche manuelle Client-Konfiguration entfällt. Die DNS-Zonendatei (Listing 1) befindet sich anschließend in */tmp* und lässt sich von dort auf dem zuständigen DNS-Server einbinden.

Zu den weiteren Komponenten, die das FreeIPA-Setup der Version 1.x installiert und konfiguriert, gehören NTP, Red Hat Directory Server, MIT Kerberos, Apache/Turbogears sowie die SELinux Targeted Policy. Dabei fragt die Setup-Routine die notwendigen Informationen wie LDAP Base DN, Kerberos Realm, Servername et cetera ab und schon nach wenigen Minuten ist der Server inklusive aller Komponenten einsatzbereit. Aufrufe von *kinit* zum Anfragen und *klist* zum Anzeigen eines Kerberos-Tickets beweisen dies, Listing 2 zeigt die Ausgaben.

Möchte man im IPA-Server Directory nach einem bestimmten Benutzer suchen, so geschieht dies mit dem folgenden Aufruf:

```
# ipa-finduser admin
cn: Administrator
homedirectory: /home/admin
loginshell: /bin/bash
uid: admin
```

Nach einer schon mit Kerberos authentifizierten Abfrage

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

des Directory-Servers listet dieser, wie in Listing 3 zu sehen, alle bekannten Attribute des Benutzers *admin* auf. Neue Benutzer lassen sich dem Directory/Kerberos-Server ebenfalls leicht hinzufügen. Der Aufruf *ipa-adduser -f Thorsten -l Scherf tscherf* fragt zweimal nach dem Passwort und bestätigt den Erfolg der Aktion mit der Meldung: *tscherf added successfully*.

Dabei kann *ipa-adduser* alle notwendigen LDAP-Attribute als Optionen übergeben. Lässt man sie weg, benutzt das Tool gewisse Defaults, wie die Ausgabe von *ldapsearch* in Listing 3 zeigt.

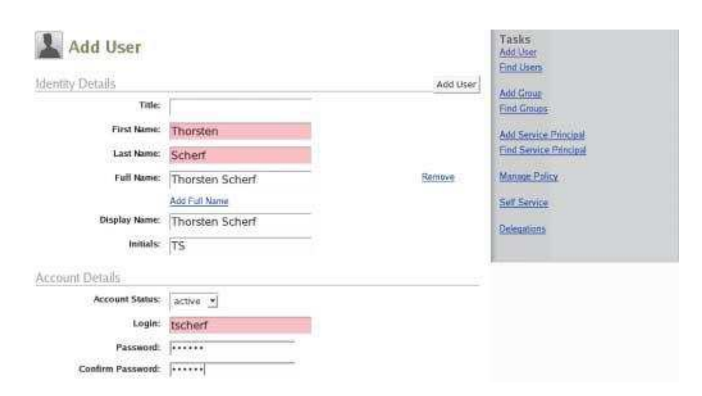
Wer zur Interaktion mit dem Directory lieber das Webfrontend verwendet, muss zunächst seinen Browser anpassen. Firefox zeigt die aktuellen Konfigurationseinstellungen via „about:config“ an. Folgende Direktiven muss man anpassen:

```
network.negotiate-auth.trusted-uris ↵
                         .example.com
network.negotiate-auth.delegation- ↵
                    uris .example.com
network.negotiate-auth.using-native- ↵
                          gsslib true
```

Baut der Admin im Anschluss eine Verbindung zum Apache-Webserver auf, begrüßt ihn ein nettes Web-Interface. Dort kann er, wie im nbentehenden Screenshot zu sehen, komfortabel Benutzer einrichten beziehungsweise das Directory abfragen sowie andere Einstellungen vornehmen.

Client-Konfiguration in Fedora

Als IPA-Client-Systeme lassen sich nicht nur Fedora und Red Hat Enterprise Linux (RHEL) konfigurieren, sondern auch viele Unix-Varianten wie Solaris, AIX, HP-UX oder Mac OS X. Sogar für Windows existiert ein eigener Client-Installer. Der folgende Abschnitt beschreibt die Konfiguration eines Fedora-Client Eine Konfigurationsanleitung für alle anderen Systeme findet sich unter [6].



Über das Web-Interface lassen sich bequem Benutzer zum Directory hinzufügen (Abb. 3).

Benutzt der Client die regulären Fedora-Repositories, so reicht zur Installation der Aufruf *yum install ipa-client ipa-admintools*. Der Aufruf *ipa-client-install* startet das Installationsprogramm, Listing 4 zeigt dessen Bildschirmausgabe.

Damit der Kerberos-Client in Zukunft beim DNS-Server nach dem richtigen Kerberos-Realm und Server fragt, sind die Anweisungen *dns_lookup_realm* und *dns_lookup_kdc* in */etc/krb5.conf* auf „true“ zu setzen. Damit ist die Konfiguration des Clients schon komplett. Benutzer können sich an diesem System nun mit den zentral verwalteten Konten anmelden. Für einen ersten Test lässt sich wieder auf *kinit* zurückgreifen, sonst klappt auch ein reguläres Login auf der Konsole per *pam_ldap* und *pam_krb5*.

Kerberos-Principals für die Dienste

Möchte man nun zusätzlich zu den Benutzerpasswörtern auch Passwörter für Services in der Kerberos-Datenbank speichern, so lässt sich dies ebenfalls einfach erledigen. Zum Erzeugen eines Kerberos-Principal für einen NFS-Server reicht der dort aufgerufene Befehl *ipa-addservice nfs/nfs.example.com*.

Damit der NFS-Server sein eigenes Passwort kennt und somit alle an ihn gerichteten Kerberos-Anfragen dekodieren kann, ist das Passwort aus der Kerberos-Datenbank des IPA-Servers auf den NFS-Server zu übertragen. Auch hierfür reicht ein einzelner Befehl:

```
# ipa-getkeytab -s server1 -p ↵
          nfs/nfs.example.com -k ↵
                  /etc/krb5.keytab
Keytab successfully retrieved and ↵
         stored in: /etc/krb5.keytab
```

Grundschutz-Forderungen

Vom BSI stammt eine umfangreiche Sammlung von Katalogen zum Thema Grundschutz [g], die sich sehr detailliert mit einzelnen Aspekten auseinandersetzen. Beispielsweise benennt der Gefahrenkatalog unter „G4 – Technisches Versagen“ als mögliches Risiko explizit den Punkt „Schlechte oder fehlende Authentikation“. Hier ein Auszug:

„Authentikationsmechanismen können zur Authentikation von Benutzern oder Komponenten oder zur Bestimmung des Datenursprungs eingesetzt werden. Wenn Authentikationsmechanismen fehlen oder zu schlecht sind, besteht die Gefahr, dass Unbefugte auf IT-Systeme oder Daten Zugriff nehmen können, die Verursacher von Problemen nicht identifiziert werden können oder die Herkunft von Daten nicht bestimmt werden kann.“

Schaut man sich den Maßnahmenkatalog etwas genauer an, so findet man beispielsweise unter dem Punkt „M5 – Kommunikation“ einen expliziten Warnhinweis vor dem Einsatz von „NIS – Network Information System“ zur Benutzerauthentifizierung in Unix-Umgebungen, da das Protokoll erhebliche Sicherheitsmängel aufweist. Aber gerade NIS findet sich noch in vielen Umgebungen, da sich viele Admins vor einem Umstieg auf LDAP wegen dessen Komplexität fürchten. Als weitere Hürde bei einem potenziellen Umstieg von NIS auf LDAP kommt erschwerend hinzu, dass zur sicheren Konfiguration eines LDAP-Servers auch die Erstellung von X.509-Zertifikaten gehört, damit die Kommunikation zwischen Client und Server verschlüsselt stattfindet und sich der LDAP-Server korrekt authentifiziert. Natürlich möchte man nun auch noch die Passwörter der Benutzer sicher verwalten und diese nicht auf einem Directory-Server ablegen. So kommt schließlich noch Kerberos ins Spiel. RAS-Benutzer (Remote Access Service) die sich via VPN in das lokale Netzwerk einwählen wollen, wurden hier noch gar nicht beachtet. Die Installation eines RADIUS-Servers (Remote Authentication Dial-In User Service) stellt also eine weitere zu lösende Aufgabe dar, wenn es um die sichere Authentifizierung von Benutzern geht. Um alle Komponenten sicher zu implementieren und zu verwalten sind schon ein immenser administrativer Aufwand sowie eine Menge Know-how notwendig.

Schaut man sich den BSI-Gefahrenkatalog weiter an, so stellt man fest, dass es mit der sicheren Authentifizierung von Benutzern ja noch lange nicht getan ist. So möchte man auch nachvollziehen können, welcher Benutzer welche Daten eingegeben hat beziehungsweise welche Aktivitäten von einem User ausgegangen sind. Das erfordert ein umfangreiches Auditing. Möchte man nun noch Sicherheitsrichtlinien auf den einzelnen Arbeitsplatzsystemen implementieren, so ist die Anzahl der hierfür notwendigen Produkte schon gewaltig und nur noch schwer zu durchschauen.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Listing 2: Ausgabe von *kinit* und *klist*

```
# kinit admin
Password for admin@EXAMPLE.COM:
# klist -5
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: admin@EXAMPLE.COM
Valid starting     Expires            Service principal
06/13/08 18:53:35  06/14/08 18:53:32  krbtgt/EXAMPLE.COM@EXAMPLE.
COM
```

Listing 3: Ausgabe von *ldapsearch*

```
# ldapsearch -Y GSSAPI uid=admin -LLL
SASL/GSSAPI authentication started
SASL username: admin@EXAMPLE.COM
SASL SSF: 56
SASL installing layers
dn: uid=admin,cn=sysaccounts,cn=etc,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: KrbPrincipalAux
objectClass: inetUser
uid: admin
krbPrincipalName: admin@EXAMPLE.COM
cn: Administrator
sn: Administrator
uidNumber: 999
gidNumber: 1001
homeDirectory: /home/admin
loginShell: /bin/bash
gecos: Administrator
memberOf: cn=admins,cn=groups,cn=accounts,dc=example,dc=com
krbLastPwdChange: 20080507084924Z
krbPasswordExpiration: 20080805084924Z
```

Listing 4: Ausgabe von *ipa-client-install*

```
# ipa-client-install
Discovery was successful!
Realm: EXAMPLE.COM
DNS Domain: example.com
IPA Server: server1.example.com
BaseDN: dc=example,dc=com
Continue to configure the system with these values? [y/N]: y
Created /etc/ipa/ipa.conf
Configured /etc/ldap.conf
LDAP enabled
nss_ldap is not able to use DNS discovery!
Changing configuration to use hardcoded server name:
server1.example.com
Kerberos 5 enabled
NTP enabled
Client configuration complete.
```

Listing 5: Daten für Replica erzeugen

```
# ipa-replica-prepare server2.example.com
Determining current realm name
Getting domain name from LDAP
Preparing replica for server2.example.com from
server1.example.com
Creating SSL certificate for the Directory Server
Creating SSL certificate for the Web Server
Copying additional files
Finalizing configuration
Packaging the replica into replica-info-server2.example.com
```

Sämtliche Informationen zur Konfiguration des IPA-Servers liegen nun im LDAP-Directory, so auch die Kerberos-Datenbank (Abb. 4).

Abschließend sei erwähnt, dass man den Kerberos-Server nun nicht mehr mit den eigenen Administrationswerkzeugen wie *kadmin* oder *kadmin .local* verwalten darf, da diese die Konfiguration des IPA-Servers zerstören würden. Der Grund hierfür sind Änderungen an der für FreeIPA verwendeten MIT-Kerberos-Implementierung. Diese legt sämtliche Kerberos-Einträge nicht mehr in einer lokalen Datei unterhalb von */var/lib/krb5kdc* ab, sondern speichert sie, wie Abb. 4 zeigt, nun ebenfalls im LDAP-Directory in einen Container mit dem Namen „Kerberos“.

Daten sind zum Replizieren da

Damit der IPA-Server nicht der Single-Point-of-Failure bei der Benutzerauthentifizierung ist, bietet es sich an, mindestens einen zweiten Master-Server (Replica) einzurichten. Bei diesem handelt es sich praktisch um einen Spiegel des IPA-Servers; jede Änderung im Directory wird hierauf repliziert. Für die Installation ist auf diesem ebenfalls das Paket *ipa-server* zu installieren. Auf der eigentlichen IPA-Maschine erzeugt der Administrator mit dem Befehl *ipa-replica-prepare* eine Datei, die alle notwendigen Informationen enthält. Listing 5 zeigt ein Beispiel. Anschließen kopiert er die so erzeugte Datei auf den zukünftigen zweiten Master-Host und startet dort die Installationsroutine. Die liest alle notwendigen Informationen nun aus der eben kopierten Datei ein:

```
server1 # scp /var/lib/ipa/replica- ↵
    info-server2.example.com root@ ↵
                  server2:/var/lib/ipa/
server2 # ipa-replica-install /var/ ↵
        lib/ipa/replica-info-server2. ↵
                            example.com
```

Ist das Installationsprogramm ohne Fehler durchgelaufen, startet im Anschluss eine Replikation der LDAP-Server-Datenbank. Verweist man in der DNS-Zonendatei auch auf den zweiten Master, stehen zwei unterschiedliche Server für Abfragen bereit. Anzumerken sei hier noch, dass in der initialen Version von IPA noch keine Synchronisation mit AD-Servern möglich ist. Jedoch sollte bei Erscheinen dieses Artikels die Version FreeIPA 1.2 verfügbar sein, die diese Funktion enthalten soll.

Fazit

Mit FreeIPA steht dem Administrator ein leistungsfähiges Werkzeug zur zentralen Speicherung von sicherheitsrelevanten Informationen zur Verfügung. Auch wenn die Version 1.x noch ganz klar auf die Speicherung von Benutzer- und Service-Identitäten ausgerichtet ist und interessante Komponenten wie Zertifikats- und Audit-Log-Verwaltung noch fehlen, lässt sich jetzt schon das große Potenzial erkennen. FreeIPA vereint viele bekannte Open-Source-Anwendungen unter einem Hut und macht deren Konfiguration und Verwaltung kinderleicht. (avr)

THORSTEN SCHERF

arbeitet als Consultant und Trainer für Red Hat EMEA und ist auf den Bereich Security spezialisiert.

Onlinequellen

[a]	BSI	www.bsi.bund.de
[b]	Likewise	www.likewisesoftware.com
[c]	FreeIPA	www.freeipa.org
[d]	Red Hat IPA	https://www.redhat.com/promo/ipa/
[e]	Dogtag	pki.fedoraproject.org/wiki/PKI_Main_Page
[f]	How to setup DNS	www.redhat.com/magazine/025nov06/features/dns/
[g]	BSI Grundschutz-Kataloge	www.bsi.bund.de/gshb/deutsch/index.htm
[h]	*iX*-Listingservice	ftp.heise.de/pub/ix/ix_listings/

Literatur

[1] Thorsten Scherf; Systemüberwachung; Schreiberling; Das Audit-Subsystem im 2.6er-Linux-Kernel; *iX* 3/2008, S. 152

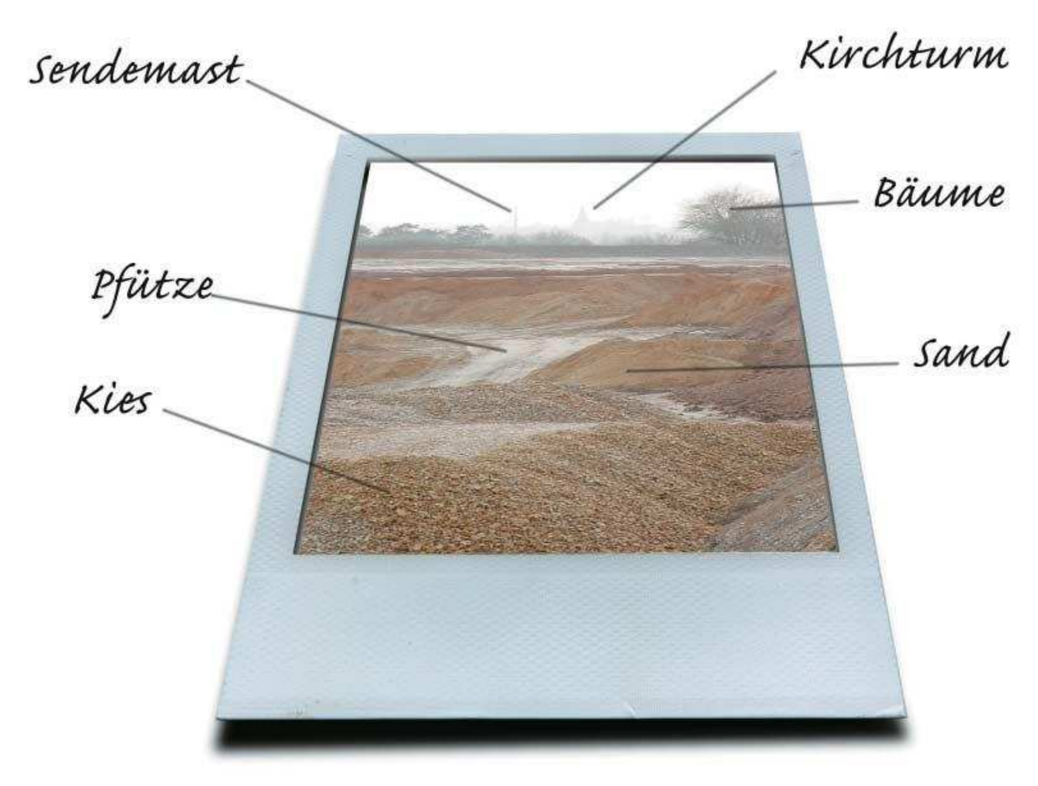
[2] Mark Pröhl, Michael Weiser; AD-Integration; Diener zweier Herren; Tutorial: Active Directory auch für Unix und Linux; *iX* 10/2008, S. 134

[3] Mark Pröhl; Michael Weiser; AD-Integration II; Völkerwanderung; Linux-/Unix-Integration via Active Directory: Freie Tools und Bordmittel; *iX* 11/2008, S. 138





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Bildannotationen im semantischen Web

Weltbeschreibung

Daniel Koch

Bildersuchmaschinen arbeiten alle nach demselben Prinzip: Man gibt einen Suchbegriff ein und bekommt mehr oder minder brauchbare Ergebnisse. Es interessiert Suchmaschinen nicht, ob „Ball“ ein Sportgerät oder eine Abendveranstaltung bezeichnet. Ein paar Produkte helfen schon jetzt, semantische Annotationen vorzunehmen.

Digitalfotos kann man gleich nach der Aufnahme im Internet präsentieren. Bildagenturen und andere bieten Fotos, Gemälde oder Digitalversionen wertvoller Schriften über professionelle Bilddatenbanken an. Wer schon Bildersuchmaschinen genutzt hat, kennt deren Grenzen: Gibt man dort „Kohl“ ein, bekommt man Fotos aus den verschiedensten Bereichen angezeigt. So präsentiert Yahoo Fotos eines Kohl-Centers, eines Baseball-Spielers gleichen Namens und des Altkanzlers Helmut Kohl in einem Fahrstuhl.

Derzeit können zwar Menschen die bereitgestellten Informationen verstehen, Maschinen sie aber nicht korrekt interpretieren. Letztere können Informationen nur lesen, wenn sie explizit vorhanden sind. Genau hier kommen Annotationen ins Spiel, denn sie können Fotos Metadaten zuweisen. Für das semantische Web sind solche Annotationen eine Voraussetzung. Mit Beschreibungssprachen wie Mikroformaten oder dem Resource Description Framework (RDF) kann man Maschinen die Bedeutung von Inhalten bis zu einem gewissen Grad „beibringen“.

Hierarchische Struktur abbilden

Das Kernkonzept von Annotationen sind Ontologien. Vergleichen lassen sie sich am ehesten mit einer Datenbank. Wie dort bilden hier Struktur und Inhalt das große Ganze. Informationen werden aber nicht einfach nur als Text in einer Datenbank gespeichert, sondern vorhandenes Wissen wird weiter interpretiert. Hat man beispielsweise die Konzepte „Karlsruhe“, „Baden-Württemberg“ und „Deutschland“ sowie die Beziehungen „Karlsruhe ist Teil von Baden-Württemberg“, „Baden-Württemberg ist Teil von Deutschland“, so kann ein semantisches System folgern, dass „Karlsruhe Teil von Deutschland“ ist. Anfragen zu „Alle Bilder aus Deutschland“ finden so auch die mit „Karlsruhe“ annotierten.

Hinsichtlich des semantischen Web stellen Ontologien semantische Modelle dar, die Daten interpretieren und zueinander in Beziehung setzen können. Und es gibt mittlerweile eine Vielzahl an Empfehlungen des World Wide Web Consortium (W3C), die sich mit dem semantischen Web befassen. Hier die wichtigsten:

– RDF [a], eine Beschreibungssprache für Informationen einer Webressource.
– OWL [b], eine Beschreibungssprache für Klassen und Relationen.
– SKOS [c], eine formale Sprache für die Kodierung von Dokumentationssprachen.
– SPARQL [d], ein Protokoll samt Abfragesprache.

Diese Ansätze bilden heute die Basis für die Arbeit am semantischen Web im Allgemeinen und Annotationen im Besonderen.

RDF als Basis des semantischen Web

Grundlage des semantischen Web ist das vom W3C entwickelte Resource Description Framework. RDF setzt sich aus vier grundlegenden Komponenten zusammen:

– Ressourcen: die mittels RDF beschriebenen Dinge – durch einen URI und eine optionale Anker-ID spezifiziert.
– Eigenschaften (Properties): Attribute oder Beziehungen, die eine Ressource genauer beschreiben.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

– Literale (Literals): können atomare Werte wie Unicode-Strings enthalten. Eigenschaften lassen sich durch Literale ausdrücken.
– Aussagen (Statements): Mit Ressourcen und Eigenschaften können in RDF Aussagen formuliert werden, indem man der Eigenschaft einer Ressource einen Wert zuweist.

Definition von Schemata

RDF ist ein Datenmodell für die Repräsentation von Metadaten, die Ressourcen beschreiben können. Allerdings kann RDF selbst nicht Strukturinformationen des generischen Konzepts definieren. Man kann daher beispielsweise nicht angeben, welche Klassen von Ressourcen es gibt. Hier kommt RDF Schema [e] ins Spiel. RDFS ermöglicht die Definition von Schemata, die Begriffe für bestimmte Einsatzgebiete in maschinenlesbarer Form festlegen. So lässt sich die Semantik von Klassen, Eigenschaften und Werten formal definieren.

RDF Schema hat, was die Ontologie anbelangt, allerdings seine Schwächen. Zwar kann es Klassen, Über- und Unterklassen sowie einfache Beziehungen abbilden, bei komplexen Beziehungen scheitert RDFS allerdings. Man kann hier zwar durchaus in die Syntaxstrukturen eingreifen, das würde allerdings zu einem nichtstandardisierten Verfahren führen, was es logischerweise zu vermeiden gilt.

Ebenfalls eine Entwicklung des W3C ist die Web Ontology Language (OWL). Mit ihr können anhand einer formalen Beschreibungssprache Ontologien erstellt, veröffentlicht und verteilt werden. OWL stellt eine Plattform für die Entwicklung themenspezifischer Vokabulare dar, mit der sich Inhalte beschreiben lassen. Dabei setzt OWL RDF und RDFS ein und nutzt zusätzliche Vokabeln, die Eigenschaften und Klassen beschreiben können. Das W3C hat es sich zum Ziel gesetzt, mit OWL die Schwierigkeiten, die bei RDF und RDFS auftauchen, zu beheben. Denn bei diesen beiden Ansätzen stand zunächst die Metadatenverwaltung im Vordergrund. Erst nachträglich erkannte man, dass sich darüber ontologische Strukturen abbilden lassen. Bei OWL stand nun exakt dieser Aspekt im Vordergrund.

SKOS, das Simple Knowledge Organisation System, ist eine auf RDF aufsetzende formale Sprache für die Kodierung von Dokumentationssprachen. Mit SKOS können semantische Strukturen beschrieben und maschinenlesbar gemacht werden. Das W3C hat SKOS als modulare und erweiterbare Sprachfamilie entworfen, deren Einsatz so einfach wie möglich sein soll.



RDFPic

Mittlerweile gibt es einige Anwendungen, die sich der genannten Techniken bedienen und Bildannotationen ermöglichen. Eine der bekannteren ist derzeit sicherlich das vom W3C in Java implementierte RDFPic [f]. In erster Linie dient es Demonstrationszwecken. Eine Fotobeschreibung setzt sich hier immer aus drei Teilen zusammen.
– Eine Beschreibung nach Dublin Core. Dabei handelt es sich um ein ursprünglich für die Erfassung von Büchern genutztes Format. In Dublin Core sind 15 Eigenschaften definiert, die zur Beschreibung von Bildern dienen können. Bei RDFPic kommen „title“, „description“, „creator“, „date“ und „type“ zum Einsatz.
– Technische Details zu Kamera, Film et cetera.
– Zusätzlich eine inhaltliche Information.

Bildbeschreibungen werden in der JPEG-Datei innerhalb der Kommentarblöcke gespeichert. Das sind Blöcke vom Typ COM, wie sie ISO DIS 10918-1 definiert. Entsprechend dem JPEG-Standard kann ein Kommentarblock beliebigen Text enthalten. Wichtig ist die Begrenzung dieser Blockgröße auf 64 KByte. Da aber wiederum die Anzahl der Blöcke unbegrenzt ist, kann man beliebig viele hinzufügen. Normalerweise geraten die von RDFPic generierten Beschreibungen aber ohnehin nicht größer als einige Hundert Byte. Wenn man zusätzlich den ebenfalls vom W3C entwickelten Webserver Jigsaw [g] verwendet, sieht ein typisches Metadaten-Beispiel im RDF-Format (von RDFPic generiert und per Jigsaw ausgeliefert) aus wie obiges Listing.



PhotoStuff

Ein weiteres Annotations-Tool ist das von der Mindswap Research Group der University of Maryland entwickelte Photostuff [h]. Mit diesem Tool können genauso wie bei RDFPic Ontologien eingesetzt werden, um den Inhalt von Bildern besser zu beschreiben. Dabei ermöglicht es dieses Tool, jedes Bildteil zu nehmen und mit Ontologien (RDF oder OWL) auszustatten. Im Vergleich zu RDFPic wirkt Photostuff deutlich weiter entwickelt.

Der Ablauf für die Bildannotation ist immer gleich. Nach dem Bild lädt Photostuff die Ontologien. Dabei kann die Ontologie-Datei eine physikalische URL sein oder auf der lokalen Festplatte vorliegen. Anschließend muss man die für die Medienliste und das Suchen verwendete Datenbank einstellen. Jetzt kann man die Bildbeschreibungen hinzufügen. Das geht leicht, indem man eine Klasse vom Klassen-Baum auf das Bild zieht. Das erzeugt eine neue In-

Listing: RDFPic-Daten

```
<?xml version='1.0' encoding='ISO-8859-1'?>
  <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
      xmlns:rdfs="http://www.w3.org/TR/1999/PR-rdf-schema-19990303#"
      xmlns:s0="http://www.w3.org/2000/PhotoRDF/dc-1-0#"
      xmlns:s1="http://www.w3.org/2000/PhotoRDF/technical-1-0#"
      xmlns:s2="http://sophia.inria.fr/~enerbonn/rdfpiclang#">
    <rdf:Description rdf:about="">
      <s0:creator>Bert Bos</s0:creator>
      <s0:relation>Marian in the Tarn</s0:relation>
      <s0:rights>Bert Bos</s0:rights>
      <s0:type>image</s0:type>
      <s0:identifier>990621</s0:identifier>
      <s0:coverage>Montredon-Labessonié (Tarn)</s0:coverage>
      <s0:date>1999-06-26</s0:date>
      <s1:camera>Canon Eos 5</s1:camera>
      <s2:xmllang>en</s2:xmllang>
      <s0:title>Marian with sheep</s0:title>
      <s0:subject>Landscape, Animal</s0:subject>
      <s0:publisher>Bert Bos</s0:publisher>
      <s0:description>Marian brings the sheep to the field in the morning. The lamb she
                                        carries was born that night.</s0:description>
      <s0:format>image/jpeg</s0:format>
    </rdf:Description>
  </rdf:RDF>
```

iX-TRACT

- Damit Rechner die Bedeutung dessen, was auf einer Abbildung zu sehen ist, extrahieren können, müssen diesbezügliche Informationen explizit vorhanden sein.
- Mikroformate und das Resource Description Framework (RDF) bilden das Gerüst für semantische Webanwendungen, die Web Ontology Language die hierarchische Struktur.
- Photostuff und Imagenotions bieten Werkzeuge wie RDFPic, erste Hilfe bei der Erstellung von Annotationen zu Bildern.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

stanz des spezifizierten Klassentyps. Sollte es innerhalb des Bildes einzeln zu beschreibende Regionen geben, greift man ebenfalls auf den Klassen-Baum zurück. Anschließend lässt sich die Annotation im RDF-Format speichern.

Momentan lassen sich in Photostuff ausschließlich Bilder in Formaten wie JPEG, PNG oder GIF laden. In Zukunft soll das Tool außerdem Video- und Audiodateien unterstützen. Eine interessante Funktion verbirgt sich im Menüpunkt Bookmarks. Hierüber können Anwender Lesezeichen auf Ontologien und Bilder setzen, um auf diese schneller zuzugreifen. Ebenfalls für die bessere Bedienbarkeit haben die Entwickler eine Suchfunktion integriert. Nach der Eingabe eines Schlüsselbegriffs können die Labels und IDs aller Instanzen und Bilder, die in der aktuellen Datenbank enthalten sind, durchsucht werden. Einige Medientypen wie JPEG können Metadaten in ihren Headern enthalten. Die bekannteste Anwendung dafür dürften sicherlich Informationen wie Datum und Uhrzeit einer Aufnahme sein. Sobald man ein Bild, das solche Metadaten besitzt, in Photostuff lädt, liest es diese Informationen aus und fügt sie in die Annotation des Bildes ein.

Leider lässt die Bedienungsfreundlichkeit zu wünschen übrig. So funktioniert das Ganze zwar recht gut, wenn man sich innerhalb einer Instanz bewegt, wenn aber eine andere Instanz hinzukommen soll, muss die zunächst angelegt werden. Das freilich setzt vom Anwender einiges an Wissen voraus. Zumindest muss er verstehen, was Instanzen, Klassen und Klassen-Bäume sind. Damit Photostuff auf dem Server läuft, müssen dort Python, die Berkeley DB und Apache installiert sein. Eine ausführliche Konfigurationsbeschreibung gibt es auf der Entwicklerseite – außerdem eine Bedienungsanleitung.



Imagenotion

Zu den Protagonisten der Bildannotationen gehört das Forschungszentrum Informatik Karlsruhe (FZI, [i]). Andreas Walter und Gabor Nagypal entwickeln das System Imagenotion [j], das schon jetzt zeigt, in welche Richtung sich Bildannotationen im Allgemeinen und Bildersuchmaschinen im Speziellen entwickeln können.

Für die Beschreibung ganzer Bilder und Bildausschnitte werden sogenannte Imagenotions erzeugt. Diese sind ein Satz elektronischer Etiketten, die die Software automatisch zu einer elektronischen Karteikarte zusammenfasst. Imagenotions beschreiben semantische Konzepte visuell. Sie bestehen jeweils aus einem Bild und mehreren Textetiketten. So kann man für die Person „Javier Solana“ eine Imagenotion erstellen, die ein sie charakterisierendes Bild zusammen mit den Textetiketten „Javier Solana“ und „Solana“ enthält. Diese Imagenotion kann mit weiteren in Beziehung gesetzt werden. Die so erstellten Imagenotions lassen sich zur semantischen Annotation von Bildern nutzen.

Im Fall von Solana könnte man die Imagenotion „Javier Solana“ mit den anderen wie „Person“, „Europäische Union“, „Generalsekretär“ und „Europa“ verbinden. Weiterhin ließe sich „Generalsekretär“ mit „Beruf“ verbinden und so ausdrücken, dass Javier Solana der Generalsekretär der Europäischen Union ist.

Finde den Generalsekretär

Zur Annotation wird zunächst ein relevanter Bildausschnitt mit einem Ausschnittsrahmen markiert und mit der entsprechenden Imagenotion verbunden. Angenommen, es gibt ein Foto einer Personengruppe, auf der unter anderem Javier Solana zu sehen ist. In diesem Fall wäre der Bildausschnitt, der das Gesicht von Javier Solana zeigt, mit der Imagenotion „Javier Solana“ verbunden.

Diese Vorgehensweise erleichtert einerseits die Annotation und verbessert gleichzeitig die Suchergebnisse. So reicht es beispielsweise Bilder, die Javier Solana zeigen, mit der Imagenotion für diese Person zu annotieren. Gleichzeitig wird dieses Bild bei Suchanfragen für „EU Generalsekretär“ ebenfalls gefunden.

In diesem Zusammenhang kommt ein weiterer Vorteil solcher Systeme zum tragen: das Handling der Mehrsprachigkeit. Die lässt sich bei Imagenotion – anders als bei vergleichbaren Lösungen – einfach realisieren. Denn hier können jedem Ontologieelement Synonyme auch in anderen Sprachen zugeordnet werden.

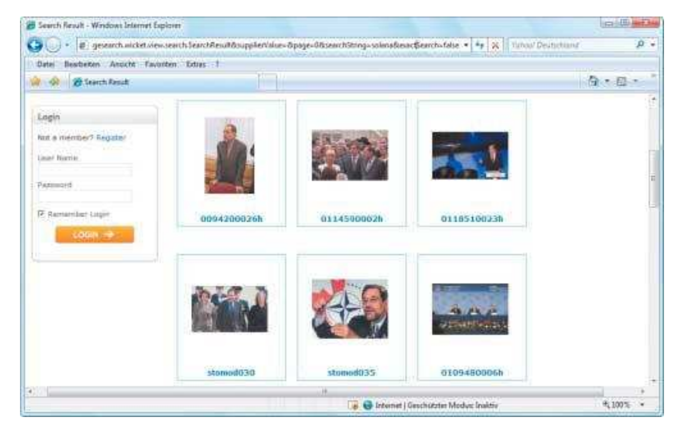
Eine wichtige Frage ist, wie diese Annotationen verwendet werden. Zusätzlich zur klassischen Bildsuche sollten die Benutzer mit einfachen Mausklicks zwischen verschiedenen Bildern navigieren können. Mit anderen Worten möchte ein Projekt wie Imagenotion ein sogenanntes Image Web schaffen, in Analogie zum World Wide Web, wo die Benutzer zwischen den Webseiten durch Mausklicks navigieren. Im Fall von Javier Solana könnte das so aussehen, dass dem Benutzer ein Bild mit verschiedenen EU-Staatschefs angezeigt wird, auf denen unter anderem der EU-Generalsekretär zu sehen ist. Klickt man auf den Solana-Bildteil, erscheinen alle Bilder, die Solana im Kontext der Europäischen Union zeigen.

In klassischen semantischen Systemen bleibt die Ontologieentwicklung getrennt von der eigentlichen Annotation. In Imagenotion wird ihre Erstellung dagegen im Annotationsprozess eng integriert. Immer wenn bei der Annotation eine Imagenotion fehlt, kann der Benutzer eine neue erstellen.

Metadaten per Drag & Drop

Das System verwendet Web-2.0-Techniken, um eine benutzerfreundliche Schnittstelle zu schaffen und bietet hierfür Funktionen wie Drag & Drop sowie Autocomplete an. So lassen sich etwa Bildannotationen per Drag & Drop erstellen.

Zusätzlich zur manuellen Annotation bietet das System eine automatische Annotationsgenerierung. Imagenotion wird hierzu in dem vom FZI geleiteten EU-Projekt Imagination [k] erweitert. Ziel des Projekts ist die weitgehende Automatisierung der

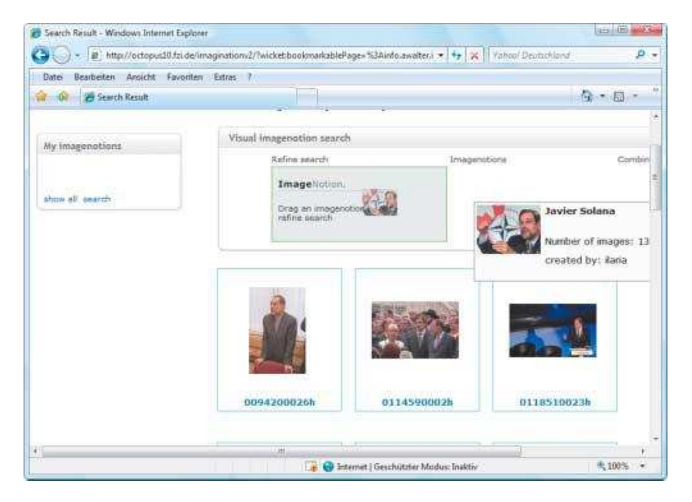


Mehrere Ergebnisse für die Suchzeichenkette „Solana“ (Abb. 1)

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Imagenotions ermöglicht das Anlegen von Annotationen per Drag & Drop (Abb. 2).

Erstellung semantischer Annotationen. Die Projektpartner bringen Techniken der Bereiche Gesichtserkennung und -identifizierung, Objekt- und Personenerkennung sowie Texterkennung ein.

Die Kombination dieser Techniken hat das FZI in Imagenotion integriert. Nach dem Laden von Bildern (oder bei manuellem Start des Annotations-Prozesses) werden semantische Informationen automatisch erstellt. Die gesammelten Informationen können Anwender manuell verfeinern oder gegebenenfalls korrigieren. In dieser automatischen Annotation liegt ein großer Vorteil von Imagenotion. Denn die größte Schwierigkeit bei anderen Verfahren ist es nun mal, dass die Annotierung von Hand erfolgen muss. Hier kann Imagenotion dem Menschen zumindest teilweise die Arbeit abnehmen. Das aber ändert nichts an der Tatsache, dass auch bei Imagenotion nach wie vor der kategorisierende Mensch vorausgesetzt wird.

MPEG-7

Außer Anwendungen wie den hier vorgestellten gibt es herkömmliche Bild- und Multimediaformate für die Annotation. Klassische Grafik- und Multimedia-Formate lassen sich, das haben die vorgestellten Anwendungen gezeigt, durchaus annotieren. Sie unterliegen aber verschiedenen Restriktionen. Ein neuer Standard war deshalb erforderlich.

2002 hat die Moving Picture Experts Group MPEG-7 [l] verabschiedet. Das Multimedia Content Description Interface, so der eigentliche Name des Standards, beschreibt multimediale Daten mit in einem oder mehreren XML-Dokument(en) gespeicherten Metainformationen. Dieses neue Format ist schon vor dem Hintergrund der Annotation von Bildern, Videos und Musik entstanden. Die in MPEG-7 definierten Beschreibungen bestehen aus Deskriptoren und Strukturen. Erstere enthalten die Merkmale der audiovisuellen Daten. Eingebettet sind Deskriptoren in Strukturen, die ihnen einen Kontext zuweisen.

Zur Definition von Deskriptoren und Beschreibungsstrukturen dient die Description Definition Language (DDL) – eine Erweiterung von RDF, die es erlaubt, MPEG-7-Beschreibungen für die Anforderungen der jeweiligen Applikation anzupassen. Das Ziel von MPEG-7 ist eine Vereinheitlichung bei der Indizierung multimedialer Daten. Denn bisherige Beschreibungsstandards wie Dublin Core stellen Metadaten lediglich für einen kleinen Teil des Metadaten-Lebenszyklus zur Verfügung.

Insgesamt ist MPEG-7 in zehn verschiedene Sparten aufgeteilt. Das soll einen isolierten Einsatz der jeweiligen Techniken ermöglichen. Typische Bereiche sind Audiodeskriptoren (für Audiosignale), Multimedia Description Schema (eine Bibliothek von Beschreibungsstrukturen) und Systems (beschreibt das Speicherformat der MPEG-7-Dokumente). Kritiker könnten jetzt einwenden, dass aufgrund des XML-Ansatzes MPEG-7 die Nachteile (beispielsweise hoher Speicherbedarf) von XML-basierten Beschreibungen übernommen habe. Dem ist nicht so. Die MPEG-7-Entwickler haben diese Stolpersteine auf Speicherebene umgehen können, indem sie MPEG-7-Werkzeuge für die effiziente Kodierung und inkrementelle Übertragung von XML-Dokumenten integriert haben.

Fazit

Die ontologiegestützte Annotation als Voraussetzung für das semantische Web steht noch am Anfang, den Kinderschuhen ist sie aber entwachsen. Deutlich machen das zunächst die vom W3C vorangetriebenen Spezifikationen zu OWL, RDF et cetera. Dass diese Techniken heute einsetzbar sind, zeigen Tools wie RDFPic und Photostuff ansatzweise. Weiter – auch was die Marktreife anbelangt – ist man beim FZI mit Imagenotion. Das Projekt soll Mitte nächsten Jahres marktreif sein und hauptsächlich für Bildersuchmaschinen im Bereich professioneller Foto-Agenturen zum Einsatz kommen. Schon jetzt nutzen einige Imagenotion aber in der Praxis [m, n]. (hb)

DANIEL KOCH

arbeitet als freiberuflicher Entwickler und Autor.



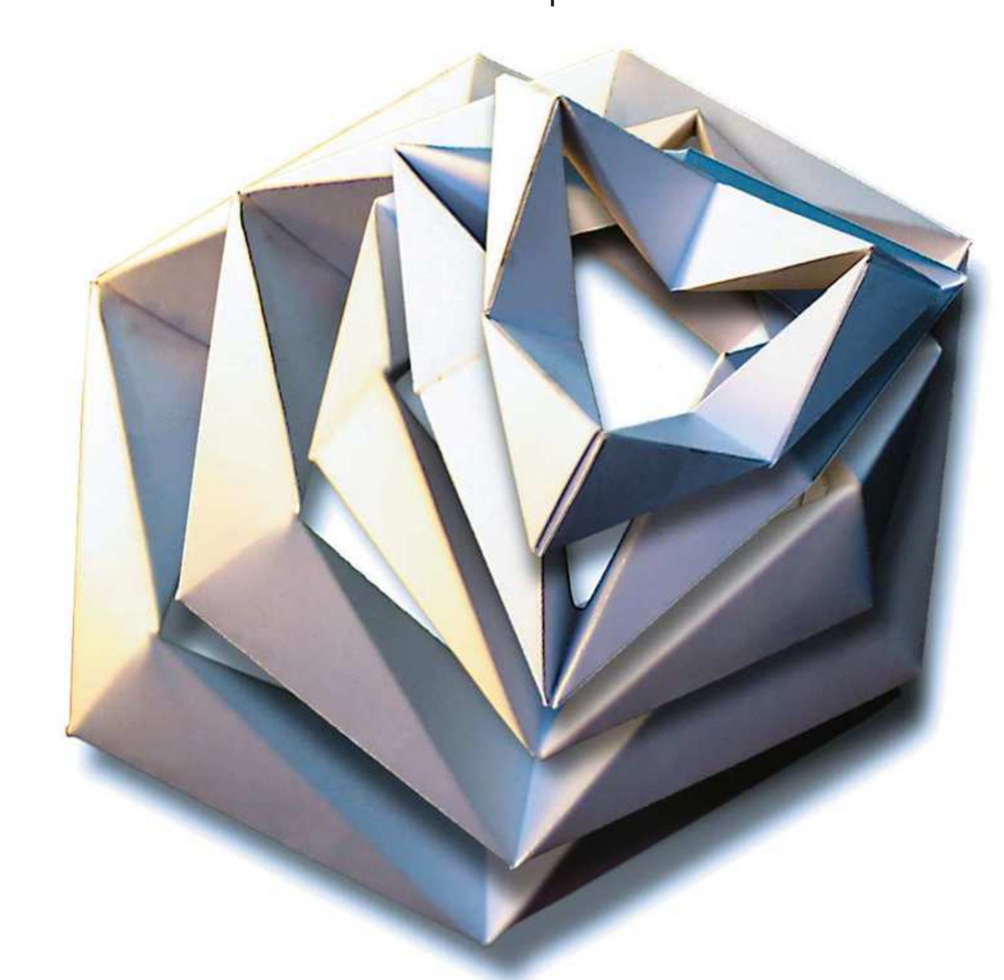


Onlinequellen

[a]	Resource Description Framework (RDF)	www.w3.org/RDF/
[b]	Überblick über die OWL Web Ontology Language	www.w3c.org/TR/owl-features
[c]	Simple Knowledge Organization System (SKOS)	www.w3.org/2004/02/skos/
[d]	SPARQL Query Language for RDF	www.w3.org/TR/rdf-sparql-query/
[e]	RDF Schema	www.w3.org/TR/rdf-schema/
[f]	RDFPic	jigsaw.w3.org/rdfpic/
[g]	Jigsaw	www.w3.org/Jigsaw/
[h]	PhotoStuff	www.mindswap.org/2003/PhotoStuff/
[i]	FZI	www.fzi.de
[j]	Imagenotion	www.imagenotion.com
[k]	Imagination-Projekt	www.imagination-project.org
[l]	MPEG-7	www.chiariglione.org/mpeg/standards/mpeg-7/mpeg-7.htm
[m]	Photo12	www.photo12.com
[n]	Deniz Saylans Homepage	www.denizsaylan.com

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Masseninfektionen mit Web Exploit Toolkits



Böse Automaten

Christoph Wegener, Dominik Birk

Seit sich Malware vom Spielzeug zum Geschäftsmodell entwickelt hat, sind auch die Wege ihrer Verbreitung immer raffinierter geworden. Der letzte Schrei sind sogenannte Web Exploit Toolkits.

Zweifelsfrei war 2007 das Jahr der Web Exploit Toolkits (WETs): Programme wie MPack, IcePack, NeoSploit und andere präsentierten die neue und äußerst effektive Art von Angriffssoftware. Mit FirePack wurde Anfang 2008 ein weiteres WET der Öffentlichkeit bekannt.

Im Geschäftsprozess rund um die Malware spielen WETs eine entscheidende Rolle, sind sie doch maßgeblich für die Infektion neuer Clients und damit den wirtschaftlichen Erfolg des gesamten Kreislaufs verantwortlich. Sie können die betroffenen Client-Systeme – meist mit Windows als Betriebssystem – beispielsweise in kriminellen Zwecken dienende Bot-Netze integrieren. Alternativ kann der WET-Server-Betreiber infizierte Client-Systeme auch an Interessierte weiterverkaufen, die diese zum Beispiel für Denial-of-Service(DoS)-Angriffe nutzen.

Lockmittel für die Clients

Bis ein Client-Rechner seinen Dienst als „Bot“ verrichtet, sind allerdings eine ganze Reihe von Schritten erforderlich. Alles beginnt mit der Infektion des Client-Rechners über den WET-Server. Beim Besuch einer entsprechend präparierten Webseite auf dem WET-Server identifiziert dieser zunächst die Browser-Version sowie das Betriebssystem des Clients und nutzt anschließend einen passenden Exploit aus – meist für eine Browser-Sicherheitslücke. Nachdem der Exploit auf dem Client beliebigen Schadcode injiziert hat, lädt Letzterer eine meist binäre Datei nach, den sogenannten Loader. Erst dieser – der zudem individuell auf das aktuelle Szenario zugeschnitten sein kann – lädt wiederum den eigentlichen Schadcode auf den Client-Rechner nach, etwa die Steuersoftware für den DoS-Angriff. Dieses Vorgehen ermöglicht es unter anderem, verteilte WET-Serversysteme zu nutzen und damit deren Entdeckung und Stilllegung erheblich zu erschweren – doch dazu später mehr.

Damit ein Angreifer einen Client-Rechner infizieren kann, muss er ihn zunächst auf einen WET-Server locken. Dazu stehen ihm verschiedene Optionen zur Verfügung. Ein probates Mittel ist die Infektion eines bekannten und stark frequentierten Webservers. Der Angreifer kann dazu entweder das WET direkt auf dem Server platzieren oder aber über die Integration eines IFrame in den Webauftritt einen weiteren Server einbinden, der dann auf das eigentliche WET verweist. Zur weiteren Verschleierung kann er sich einer ganzen Kette von IFrame-Referenzierungen bedienen, die sukzessive jeweils aufeinander verweisen.

Für die Manipulation eines Webservers muss ein Angreifer ihn zunächst unter seine Kontrolle bringen. Der Einbruch in die Server erfolgt dabei meist über eine Techniken wie „Remote File Inclusion“ (kurz: RFI) oder „Mass SQL Injection“, die an sich Stoff für einen weiteren Artikel liefern würden. Die Ursachen für deren Erfolg liegen oft in fehlerhaft geschriebenen serverseitigen Skripten. Sie er-

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

möglichen es Angreifern, eine Shell auf den Server zu bringen, die wiederum das Ausführen beliebiger Aktionen im Kontext des Webservers erlaubt. Dies sollte ein weiterer Grund sein, die Server seiner Webpräsenz – inklusive aller Webapplikationen – regelmäßig zu aktualisieren.

Daneben lassen sich Methoden wie „SEO IFrame Injection“ (SEO steht für „Search Engine Optimization“) nutzen, um den Client auf den WET-Server zu locken. Dabei nutzt der Angreifer häufig eine XSS-Schwachstelle (Cross-Site-Scripting) in einer bekannten und deshalb im Google-Ranking hoch bewerteten Webseite aus und platziert per HTTP-GET-Parameter einen IFrame darin. Gelingt dies, kann der Angreifer den URL inklusive der XSS-Schwachstelle in großem Stil publizieren. Dadurch tauchen die infizierten URLs nun aber auch im Suchmaschinen-Ranking weiter oben auf, was die Chance, von einem potenziellen Opfer aufgerufen zu werden, nochmals erhöht.

Der Kauf ähnlicher Domain-Namen, um Vertipper zu bedienen, oder der Erwerb von Suchmaschinen-Ads – quasi den kostenpflichtigen Links zu diversen Suchwörtern – sowie den Einsatz von Spam stellen weitere gängige Wege dar, die Angreifer nutzen können, um Opfer auf den kompromittierten Server zu locken.

Wie oben angesprochen, vollzieht sich die Infektion eines Client-PCs in mehreren Schritten. Wurde der Client auf den WET-Server gelockt, tritt das Exploit-Skript in Aktion – meist in Form eines PHP-Skriptes. Dieses analysiert zunächst die Version des verwendeten Browsers und des Systems, indem es etwa den „User-Agent“ auswertet. Daraus lassen sich Rückschlüsse auf die verwendete Browser-Version und damit zum Teil indirekt auf das verwendete Betriebssystem ziehen, denn ein MS Internet Explorer lässt sich unter Linux nur schwer verwenden. Eine Analyse der IP-Adresse kann außerdem Informationen über den Standort des Rechners und damit auf die Sprachversion liefern.

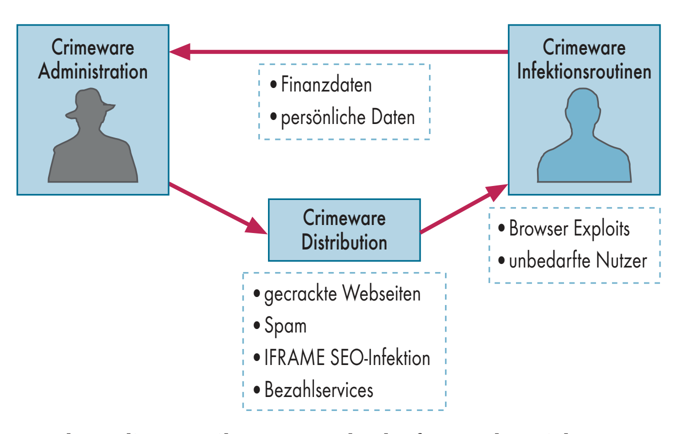
Mehrere Schritte zum Erfolg

Auf Basis der so gesammelten Daten wählt das WET den Exploit aus, überträgt ihn an den Rechner des Opfers und führt ihn dort aus. MPack und IcePack tragen den Nutzer zudem in eine Datenbank ein, FirePack legt die Daten in verschiedenen Textdateien ab. Unter diesem Gesichtspunkt ist es auch interessant, dass alle WETs Funktionen zum Blocken beziehungsweise Wiedererkennen von IP-Adressen eingebaut haben. Sie sollen verhindern, dass derselbe Client mehrfach attackiert wird.

Anschließend lädt der auf dem Client ausgeführte Exploit eine (meist) binäre Datei nach – den sogenannten Loader. Letzterer muss dabei nicht zwingend vom WET-Server stammen, sondern kann sich auf einem weiteren Host befinden. Schließlich führt der Client den Loader aus, der wiederum den eigentlichen auf dem Client auszuführenden Schadcode nachlädt. Sind alle diese Schritte erfolgreich ausgeführt, ist der Client infiziert und fungiert von nun an ganz im Sinne des Angreifers.

iX-TRACT

- Die Verbreitung von Malware hat sich inzwischen vom Spielzeug zum Geschäftsmodell entwickelt.
- WETs – Web Exploit Toolkits – sind das aktuelle Mittel der Wahl für die Infektion von Rechnersystemen.
- Diverse Verschleierungsmethoden erschweren die Erkennung von WETs außerordentlich.



Rund um die Verteilung von Schadsoftware hat sich unter dem Schlagwort Crimeware ein einträgliches Geschäftsmodell etabliert (Abb. 1).

Ein Vergleich des Bösen

Im weiteren Text folgt eine Gegenüberstellung der drei bekannten WETs MPack, IcePack und FirePack. MPack vom „Dream Coders Team“ ist dabei das „älteste“ WET, das schon seit 2006 im Internet kursiert. Das 2007 entdeckte IcePack von der „IDT Group“ stellte erstmals eine IFrame-Funktion in einem WET zur Verfügung. FirePack, über dessen Urheber nichts bekannt ist, tauchte für die breite Öffentlichkeit sichtbar Anfang 2008 auf, es liegen aber durchaus Hinweise vor, dass es schon im Jahre 2007 im Einsatz war.

Zudem lässt sich feststellen, dass für die drei WETs völlig unterschiedliche Preise gelten. Während MPack zu Preisen zwischen US$ 700 und US$ 1000 gehandelt wurde, sind für IcePack etwa US$ 400 zu zahlen. Firepack hingegen fällt mit US$ 3000 etwas aus dem Rahmen. Das Preismodell an sich ist modular. So kann man beispielsweise gegen ein kleines Extra-Entgelt eine Garantie auf Nicht-Erkennung durch die gängigsten Virenscanner bekommen. Ein solches Modell ergibt vor allem deshalb einen Sinn, da sich die Skripte – und WETs sind im Grunde nichts anderes als eine Sammlung solcher – leicht kopieren lassen. Im Internet findet man daher an zahlreichen Stellen Kopien der gängigsten WETs. Interessierte seien jedoch gewarnt: Das Risiko bei der Verwendung kopierter WETs ist genauso hoch wie bei normalen Softwarekopien. Es kursieren auch Versionen von WETs, die eine zusätzliche Hintertür enthalten und somit auch den interessierten Laien zum Opfer werden lassen. Beim Experimentieren mit den WETs ist somit große Vorsicht angebracht, zudem sind natürlich auch die einschlägigen gesetzlichen Regelungen zu beachten.

Alles, was krank macht

Hat der Angreifer das Opfer auf die infizierte Webseite gelockt, muss – möglichst unbemerkt – die Infektion des Client-PC erfolgen. Dieser Prozess läuft, wie oben beschrieben, in mehreren Schritten ab. An letzter und entscheidender Stelle steht das Ausführen des für den jeweiligen Client-PC passenden Exploits. Hierzu haben alle WETs mehrere mehr oder

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

weniger alte Exploits im Gepäck. Diese beinhalten Exemplare aus völlig unterschiedlichen Bereichen: Vom Media Player, der Management Console, über Browser-spezifische Exploits für den Internet Explorer bis zu Sicherheitslücken in diversen Add-ons wie dem Yahoos Messenger sind nahezu alle Komponenten aus dem Bereich Multimedia vertreten. Die Exploits sind als „Plug-in“ in die WETs integriert. Das vereinfacht künftige Erweiterungen und bietet auf der anderen Seite dem interessierten Anwender potenziell die Möglichkeit, eigene Exploits in das Framework einzubinden.

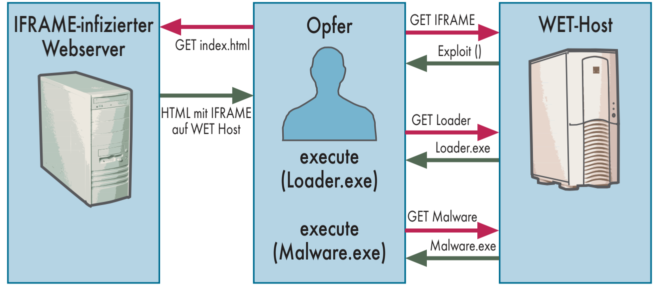
WETs begegnen gängigen Intrusion-Detection-Techniken bei der Infektion des Clients vor allem durch Kodierung des Javascript-Payloads. Diese Kodierung dient aber nicht der Geheimhaltung, denn den Schlüssel liefern die WETs direkt mit. Dieser ist allerdings meist bei jeder Auslieferung des Schadcodes neu und vor allem zufällig gewählt. Das erschwert die Analyse durch Intrusion-Detection/Prevention-Systeme sehr, denn es gibt nun keinen validen Fingerprint des Schadcodes mehr. Damit wird eine automatische Erkennung des WET-Schadcodes und seine Bekämpfung fast unmöglich.

Zur Vereinfachung der Bedienung bringen alle WETs eine mehr oder weniger ausgefeilte Verwaltungsoberfläche mit, die neben der reinen Bedienung auch statistische Aussagen erlaubt. MPack bietet dazu ein Administrations-GUI, das aus einer einzelnen Webseite besteht – aber immerhin statistische Infos dazu liefert, wie viele Clients angegriffen werden und welche Browser auf diesen Clients zum Einsatz kamen.

Bedienung leicht gemacht

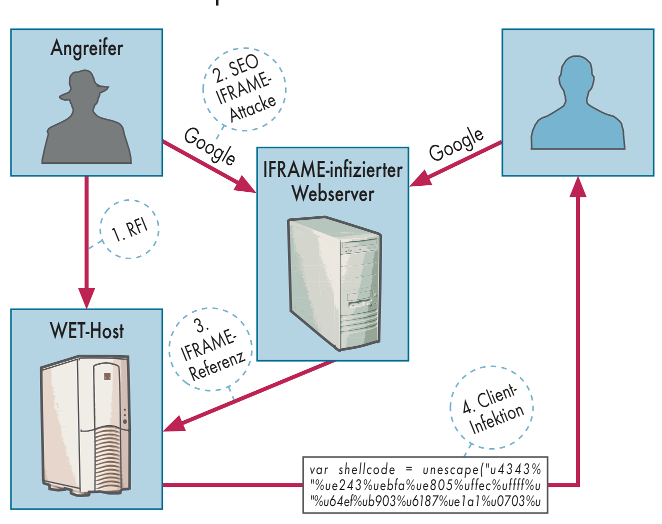
IcePack bietet dem Admin dagegen eine deutlich detailliertere Bedien- und Auswertemöglichkeit. Nach Authentifizierung empfängt dieses WET den Administrator zunächst mit einer gut strukturierten Übersichtsseite, die Systeminformationen und den Zeitpunkt des letzten Zugriffs auf das Exploit-Script anzeigt. Darüber hinaus bietet es drei Dropdown-Menus, die dem Administrator weitere Informationen liefern. Menu 1 stellt vor allem Funktionen zur statistischen Auswertung (Anzeige der Herkunftsländer der Client-PCs, Löschen der Statistiken, …) zur Verfügung. Menu 2 gibt dem Administrator eine Funktion, die bisher kein anderes WET hat: das automatisierte Ablegen von Schadcode auf Webservern. Hierzu muss man lediglich eine Datei mit „bekannten“ FTP-Zugängen bereitstellen, alle weiteren Schritte übernimmt IcePack voll automatisiert. Diese Funktion erlaubt zudem nicht nur das „IFramen“ von Webservern, sondern ist flexibel gestaltet. Im Prinzip ließe sich so auch eine automatisierte Weiterverbreitung des IcePack selbst erreichen. Menu 3 schließlich enthält noch drei kleine, nützliche Werkzeuge: Hier kann man individuellen IFrame-Code bearbeiten, einstellen, welche IP-Adressen das Toolkit blockieren soll und den Zugangscode zum Administrator-Account ändern.

Web Exploit Toolkits – Client-Infektion



Für die Client-Infektion reicht unter Umständen der einmalige Besuch einer WET-verseuchten Website aus (Abb. 2).

Web Exploit Toolkits – Infektionsroutine



Eine Infektion über ein WET erfolgt in mehreren Schritten (Abb. 3).

Obwohl das jüngste WET, bietet FirePack bei Weitem nicht die Administrationsmöglichkeiten des IcePack. Zwar bietet es auch eine statistische Analyse, darüber hinaus aber lediglich zwei weitere Funktionen. So kann der Administrator die Referer einsehen und löschen. Die Liste der zu blockierenden IP-Adressen muss man hingegen per Textdatei (*ip_ban.txt*) festlegen. Wie schon erläutert nutzt FirePack keine Datenbank, sondern legt alle Informationen in Textdateien ab. Diese Einschränkung beziehungsweise der geringe Funktionsumfang sind aber auf der anderen Seite der entscheidende Vorteil von FirePack: Eine geringe Dateigröße und eine enorme Kompaktheit der Funktionen führen zu einer hohen Effizienz.

Verteidigung ist schwer

Schutzmaßnahmen gegen professionell gemachte WETs sind nicht einfach umzusetzen. An erster Stelle sollte immer das Patchen des verwendeten Betriebssystems, des Browsers und anderer Software stehen. Hier sind möglichst unverzüglich nach Veröffentlichung alle Hersteller-Patches einzuspielen – wenn das technisch machbar ist. Und dies gilt nicht nur für die Clients, sondern erst recht für Webserver, bieten diese wie beschrieben oft überhaupt erst die Grundlage für einen erfolgreichen Angriff. Dabei darf man allerdings nicht vergessen, dass Angreifer immer mehr Zero Day Exploits ausnutzen, sich also Schwachstellen bedienen, die weder dem Hersteller noch der Allgemeinheit bekannt sind. Dagegen hilft dann auch Patchen nicht mehr, schlicht und ergreifend deswegen, weil zumindest in einem mehr oder weniger großen Zeitfenster kein Patch zur Verfügung steht.

Neben einem System auf aktuellem Stand kann man Techniken einsetzen, die die Ausführung von Javascript-Code auf dem Client verhindern, oder zumindest deutlich einschränken. Die Firefox-Extension „NoScript“ bietet dazu ein kostenloses Werkzeug, dass die Ausführung von JavaScript-Code nur für vertrauenswürdige Webseiten erlaubt. Hat der Angreifer aber eine (ehemals) vertrauenswürdige Webseite unter seine Kontrolle gebracht, ist auch hier der Erfolg der Maßnahmen stark eingeschränkt. Hinzu kommt, dass viele Webseiten heute

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

einfach auf Javascript bauen – eine breit gestreute Akzeptanz dieser Abwehrmethode ist somit ebenfalls fraglich.

Eine weitere Option ist die Verschleierung der verwendeten Version des Webbrowsers. Da der Erfolg des Exploits in vielen Fällen von der Kenntnis der verwendeten Browsers abhängt, kann man den Angreifer hier zumindest so verwirren, dass er den falschen Exploit anwendet und der Angriff damit ins Leere läuft. Allerdings dürfte es – falls sich diese Schutzmaßnahme durchsetzen sollte – nur eine Frage der Zeit sein, bis sich die Angreifer darauf eingestellt haben. Durch wahlloses Testen könnten sie diesen Schutz schnell umgehen. Zudem darf man nicht verschweigen, dass diese Maßnahme die Benutzbarkeit im Alltag des Web einschränken kann.

Schließlich würde das Blocken von IP-Adressen, die als Malware-Verbreitungsweg bekannt sind, einen kleinen zusätzlichen Schutz bieten. Wie alle Blacklist-Ansätze steht und fällt dies mit der Aktualität und birgt Risiken eines Denial of Service (DoS) gegen Unbeteiligte. Im Zeitalter von Bot-Netzen und FastFlux ist der Erfolg von Blacklisting in Bezug auf die obigen Punkte zudem erst recht als wenig erfolgversprechend einzustufen.

Während die bisher genannten Maßnahmen eher auf dem PC des Anwenders stattfinden, existieren seit einiger Zeit Produkte, die sich eines zentraleren Ansatzes bedienen. Die auch Web-Reputationsfilter genannte Methode verwendet einen Blacklist-Ansatz: Fragt der Nutzer eine URL an, prüft der Filter zunächst in Echtzeit, ob die betreffende URL auf einer Blacklist steht. Falls ja, warnt er den Nutzer oder – je nach Einstellung – verwehrt ihm den Zugang vollständig. Bei der Anfrage einer bisher unbekannten URL versucht das System hingegen aus mehreren Parametern, wie den Daten des Registrars, der Frequentierung der URL und anderen, eine Wertung (Scoring) für die „Gesundheit“ dieser URL zu bestimmen. Allerdings ist das System mit den für Blacklist-Ansätze typischen Schwächen, wie dem ungewollten Denial-of-Service Unbeteiligter, behaftet.

Was bringt die Zukunft?

WETs erfreuen sich großer Beliebtheit in der Crimeware-Szene, denn damit lassen sich extrem effektiv Client-PCs angreifen. Für den Nutzer stellt diese neue Art der Malware-Verbreitung eine enorme Gefahr dar. Allein der Besuch einer Webseite reicht unter Umständen dazu aus, dass der Nutzer seinen Client-Rechner völlig unbemerkt mit Malware infiziert und ihn in einen ferngesteuerten Bot verwandelt. WETs dürften in Zukunft weiter an Bedeutung gewinnen. Vor allem die steigende Durchdringung der neuen Fähigkeiten des Web-2.0 erschließt den Angreifern völlig neue Möglichkeiten.

Zudem hat die Vergangenheit gezeigt, dass die WET-Betreiber schnell auf veränderte Bedingungen reagieren, die Entwicklungen im Bereich SEO-IFrame-Infektion sind nur ein Beispiel dafür. Auch das Javascript-Toolkit, das über die Manipulation des Title-Tag innerhalb von kürzester Zeit mehr als 10 000 Webseiten infizierte, ist unter diesem Gesichtspunkt interessant. Sein besonderer Clou: Es speichert die IP-Adressen der gängigen Suchmaschinen und liefert bei deren Anfragen „sauberen“ Code zurück. Greift aber ein potenziell verwundbarer (privater) PC auf die Seite zu, so tritt das Script in Aktion und versucht eine ganze Reihe von Exploits auszuführen. Zudem bedient sich das Javascript-Toolkit mehrerer Mechanismen zur Verschleierung – was vor allem die Erkennung durch Standard-Anti-Virus-Software erheblich erschwert.

Web Exploit Toolkits – Host-Infektion

components/com_artlinks/artlinks.dispnew.php?mosConfig_absolute
index2.php?x= inurl:index2.php?x=*.php"
main.php?pagina= inurl:"main.php?pagina=*.php"
test.php?page= allinurl:test.php?page=
components/com_phpshop/tollbar.phpshop.html.php?mosConfig_absolute
Google Dorking
WET-Host
PHP Shell (r57,c99 ...)
WET Software

Bei einer Host-Infektion spielen oft fehlerhaft geschriebene serverseitige Skripte eine unrühmliche Rolle (Abb. 4).

Fazit

Malware ist definitiv kein Spielzeug mehr, sondern hat sich zu einem sehr ertragreichen Geschäftsmodell entwickelt. Daher verwundert es nicht, dass auch die Angreifer immer neue und effizientere Wege zur Verbreitung ihres Schadcodes suchen. WETs stellen momentan wohl einen beliebten, weil sehr effektiven Weg für einen Angreifer dar. Dies gilt vor allem, weil aus Sicht des Opfers schon der einmalige Besuch einer verseuchten Webseite zur Infektion des eigenen Rechners ausreichen kann – und das Ende der Fahnenstange scheint in Bezug auf die Möglichkeiten der Angreifer noch lange nicht erreicht. Eine Abwehr dieser Form von Malware gestaltet sich zudem nicht einfach, denn viele Maßnahmen lassen sich aus Sicht der Angreifer einfach umgehen. Eines steht dadurch aber jetzt schon fest: Es bleibt spannend im Rennen zwischen Angreifer und Verteidiger. (avr)

Onlinequellen

Masseninfektionen von seriösen Webseiten
www.heise.de/newsticker/meldung/106959/

Hack der „Miami Dolphins“-Website
www.heise.de/newsticker/meldung/84761/

Remote File Inclusion
en.wikipedia.org/wiki/Remote_File_Inclusion

Hintergründe zum IcePack
pandalabs.pandasecurity.com/blogs/images/PandaLabs/2007/12/18/Icepack.pdf

Infos zum Javascript-Toolkit
www.0x000000.com/index.php?i=534

CHRISTOPH WEGENER

CISA, CISM und CBP, ist promovierter Physiker und seit 1999 mit der wecon.it-consulting freiberuflich im Thema IT-Sicherheit aktiv. Zudem ist er am Horst Görtz Institut für IT-Sicherheit in Bochum tätig.

DOMINIK BIRK

ist Autor zahlreicher Fachartikel, Gewinner des letztjährigen „Best Student Paper Award“ des BSI und freiberuflich im IT-Sicherheitsumfeld aktiv.

Literatur

[1] Wilhelm Dolle, Christoph Wegener; Malware II; Fieberwarnung; Funktion und Nutzen von Web-Reputations-Filtern; *iX* Special Sicher im Netz; Herbst 2008, S. 34





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Streaming mit dem VLC-Player

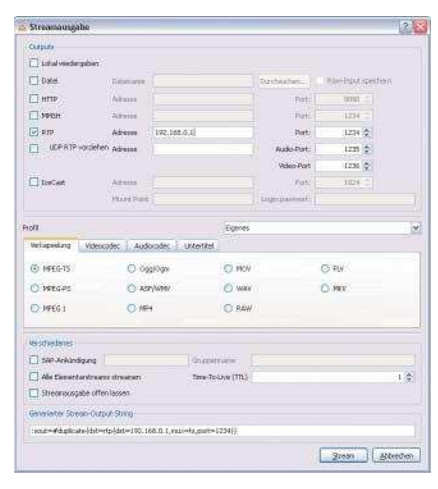
Sendestation

Horst Eidenberger

Audio- und Videodatenströme ins Netz zu senden, ist keine Zauberkunst. Dazu muss man nicht mal einen Server einrichten: Der VLC-Player enthält alle Funktionen, die man zum Streamen braucht.

Im Äther ist das Verbreiten eigener Inhalte lizenzierten Sendern vorbehalten. Im Netz hingegen darf es jeder. Mit der geeigneten Software lässt sich im Handumdrehen ein eigenes Programm auf die Beine stellen – etwa mit dem VLC-Player des VideoLAN-Projektes (siehe Kasten „Onlinequellen“). Er ist für zahlreiche Betriebssysteme erhältlich, darunter Linux, Mac OS X und Windows. Wer ein BSD, Solaris oder QNX einsetzt, muss den Quelltext allerdings selbst übersetzen.

Der VLC-Player ist als Einzelanwendung nutzbar, aber auch als Browser-Plug-in oder Entwicklungsumgebung für eigene Medienverarbeitungs-Anwendungen. Er unterstützt alle wichtigen Codecs – darunter MPEG-4 Part 2 und Part 10 (H.264), Sorensen und Windows Media Video (WMV) – und Containerformate (siehe den Artikel „Turbulente Strömungen“ auf Seite 114). Darüber hinaus bringt er Ein- und Ausgabefilter für DVB-Datenquellen, HTTP- und FTP-Download sowie fast alle Streaming-Formate mit – einschließlich Microsofts MMS.



Sendezentrale: Alle Streaming-Parameter lassen sich in einem Dialog einstellen. Vorgefertigte Profile erleichtern das Auswählen der Codecs und Containerformate.

Ü-Wagen auf dem Desktop

Beim Schritt zur aktuellen Version 0.9.2 haben die Entwickler einige Änderungen an der Benutzeroberfläche vorgenommen. Denen fiel leider auch der „Streaming-Assistent“ zum Opfer, der Nutzer in wenigen, einfachen Schritten zum Erfolg führte.

Wählt der Nutzer den Menüpunkt „Medien/Streaming“, muss er zunächst den zu sendenden Datenstrom auswählen. Das Programm kann Dateien, CDs und DVDs öffnen oder Live-Streams aus dem Netz empfangen und weitergeben (Relais-Funktion). Die Windows- und Linux-Versionen erlauben es außerdem, auf angeschlossene Geräte wie DVB-Empfänger oder Kameras zuzugreifen. In welchem Format die Daten vorliegen, spielt dabei keine Rolle: Der VLC-Player führt alle notwendigen Konvertierungen automatisch durch.

Anschließend kann man im Streaming-Dialog die Versandart wählen (siehe Abbildung). Für Video-Streaming eignet sich am besten das in RFC 3550 definierte Real-Time Transport Protocol (RTP). Will der Nutzer nur einen Rechner beschicken, muss er dessen IP-Adresse eingeben. Sollen mehrere das hausgemachte Programm empfangen können, muss man eine Multicast-Adresse aus dem Bereich *225.0.0.0* bis *238.255.255.255* eintragen – die Adressbereiche *224.0.0.0/8* und *239.0.0.0/8* sind überwiegend für Spezialanwendungen wie Routingprotokolle reserviert und damit für den Anwender tabu.

Zudem ist es im Multicast-Betrieb unerlässlich, die Sendereichweite einzuschränken. Dazu dient der Time-To-Live-Parameter (TTL): Er bestimmt, wie viele Router die Datenpakete maximal überspringen dürfen („hop count“). Generell sollte man den Wert so niedrig wie möglich wählen. Der voreingestellte Wert *1* stellt sicher, dass der Medienstrom das lokale Netz nicht verlässt.

Unter „Profil“ muss der Nutzer eins der vordefinierten Sendeformate einstellen, etwa MPEG-2 oder H.264. Wählt er „Eigenes“, kann er das Containerformat („Verkapselung“) und die verwendeten Codecs und Formate für Audio, Video und Untertitel – sofern vorhanden – separat bestimmen.

Soll der VLC-Player als Empfänger dienen, muss der Zuschauer unter „Medien/Netzwerk öffnen“ lediglich das verwendete Protokoll – hier RTP – auswählen und die korrekte Adresse einstellen: seine eigene bei Unicast-Betrieb, sonst die vom Server genutzte Multicast-Adresse. Kommt es bei der Wiedergabe zu Rucklern, empfiehlt es sich, das Kästchen „Mehr Optionen anzeigen“ zu markieren und im erweiterten Dialog die Caching-Parameter zu variieren.

Seine Vielseitigkeit und einfache Bedienung machen den VLC-Player zum idealen Instrument fürs Ad-hoc-Streaming. Wer rund um die Uhr senden will, sollte sich jedoch nach einer anderen Lösung umsehen. Eine Liste geeigneter Software ist in der englischen Wikipedia-Ausgabe zu finden. (mr)

Onlinequellen

VideoLAN-Projekt:
www.videolan.org

RTP: A Transport Protocol for Real-Time Applications:
tools.ietf.org/html/rfc3550

Streaming-Software (Wikipedia):
en.wikipedia.org/wiki/List_of_streaming_media_systems

DR. HORST EIDENBERGER

ist außerordentlicher Professor an der TU Wien und zertifizierter Gutachter am Handelsgericht Wien.





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Unix-Benutzerinformationen ins Active Directory migrieren

Völkerwanderung

Mark Pröhl, Michael Weiser

Für einen endgültigen Abschied vom antiquierten NIS soll die komplette Benutzerverwaltung inklusive der POSIX-Attribute ins Active Directory wandern. Wer keine Überraschungen wünscht, sollte dabei aber ein paar Vorsichtsmaßnahmen treffen.

Beim Unternehmen für „Neue, innovative Service- und Applikationsdienstleistungen“ (NiS-AD) läuft ein Projekt, das die Benutzerverwaltung für Unix- und Windows-Rechner vereinheitlicht. Statt wie bisher für die Unix-Welt getrennte NIS-Maps zu pflegen, sollen sämtliche Rechner ihre Nutzerinformationen künftig über ein zentrales Active Directory (AD) beziehen. In Phase eins des Projektes haben die Administratoren bereits die Systemanmeldung der Linux- und Unix-Rechner so modifiziert, dass sie nicht mehr NIS verwendet, sondern die Nutzer über das Kerberos-Protokoll am Domänen-Controller (DC) authentifiziert [1]. Die verschlüsselten Passwörter aus der NIS-Map *passwd* konnten sie damit eliminieren. Alle übrigen Informationen kommen jedoch nach wie vor aus NIS-Maps – ein Umstand, den die Administratoren nun in der zweiten Projektphase beheben wollen, bevor sie in Phase drei die Möglichkeiten des Single Sign-On über AD voll ausschöpfen.

Zwei Ziele stehen ganz obenan für das AD-Migrationsprojekt bei NiS-AD: Zum einen soll Schluss sein mit dem Mehraufwand, den zwei parallele Nutzerverwaltungen für Unix und Windows verursachen. Zum anderen haben die Auditoren einige prinzipielle Schwachstellen im NIS ausgemacht, die nicht mehr den gestiegenen Sicherheitsanforderungen an das NiS-AD-Netz entsprechen. Daher genügt es ihnen nicht, den in AD integrierten NIS-Serverdienst zu verwenden. Der würde zwar die Benutzerverwaltung vereinheitlichen, die Sicherheitsbedenken blieben jedoch bestehen – wenngleich die Administratoren durch das Entfernen der verschlüsselten Passwörter die sensibelsten Daten bereits aus den NIS-Maps getilgt haben. Konkret setzt das Funktionsprinzip von NIS ein vertrauenswürdiges Netz voraus. Andernfalls droht die Gefahr, dass ein Angreifer als Man-in-the-Middle den Datenstrom zum NIS-Server abfängt und unbemerkt verändert. Dazu muss er nur IP-Adressen oder DNS-Namen manipulieren können. In manchen – durchaus gebräuchlichen – Konfigurationen genügt sogar ein Notebook am Firmennetz, das sich als NIS-Server ausgibt und Clientrechner mit gefälschten Nutzerdaten füttert. Eine Option zur Schaffung eines derart vertrauenswürdigen Netzes wäre der flächendeckende Einsatz von IPSec im gesamten Unternehmen. Der Aufwand dafür ist jedoch ebenso hoch wie der Ressourcenhunger. Umso attraktiver erscheint die Alternative: Statt das Netz zu sichern, tauscht

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

man NIS gegen einen anderen Verzeichnisdienst, der geringere Anforderungen stellt. Das Lightweight Directory Access Protocol (LDAP) ist ein solcher Dienst, der als zentraler Bestandteil in AD integriert ist und auch für Unix flächendeckend bereitsteht. Keine Frage daher, dass die Administratoren bei NiS-AD diesen Weg gehen und ihre NIS-Infrastruktur durch eine LDAP-AD-Anbindung ablösen.

Abgleich der Detailinformationen

Dazu muss AD in der Lage sein, alle bislang im NIS gespeicherten Nutzerinformationen abzubilden. Das ist keineswegs selbstverständlich, denn beide Verzeichnisdienste verwalten ihre Daten auf unterschiedliche Weise. NIS gruppiert Informationen in einzelnen Karten (Maps), deren Namen Rückschlüsse auf die Bedeutung der enthaltenen Informationen zulassen. Ein einzelner Eintrag besteht aus einem Schlüsselwort und einem dazugehörigen Wert. Wie er zu interpretieren ist, lässt NIS offen. Das ist allein Aufgabe der Applikation, die auf die Informationen zugreift. So besteht die NIS-Map *passwd.byname* beispielsweise aus Einträgen, die dem Namen eines Benutzerkontos eine Zeichenkette mit zusätzlichen Informationen zuordnet. Dass die Zeichenkette ein spezielles Format verwendet und durch Doppelpunkt getrennt in Felder für Passwort, User- und Gruppen-ID, Beschreibung, Home-Verzeichnis und Login-Shell aufgeteilt ist, braucht NIS nicht zu interessieren. Das Auswerten der Einträge übernimmt jede Applikation selbst.

AD ist anders strukturiert. Es verwaltet seine Daten in einem Format, dessen Entwurf ursprünglich für den Verzeichnisdienst X.500 entstand. Es gruppiert zusammengehörige Einträge zu Objekten, die selbst hierarchisch in eine Baumstruktur eingegliedert sind. Sogenannte Schemadefinitionen legen fest, welche Einträge erlaubt sind, welchen Typ und welche Bedeutung sie besitzen. Zwar lassen sich prinzipiell NIS-Map-Einträge direkt als Schlüssel-Wert-Paare in einzelne X.500-Objekte abbilden, doch dabei bleiben all die Vorteile auf der Strecke, die der typisierte, objektorientierte Aufbau im Vergleich zu NIS bietet. Verwendet man stattdessen für jeden Eintrag aus der *passwd*-Map ein eigenes Benutzerobjekt mit separaten Attributen für User-ID, Home-Verzeichnis et cetera, benötigen einzelne Applikationen keinen eigenen Parser mehr. Darüber hinaus verhindert schon die Syntaxkontrolle des Servers, dass man beispielsweise für die numerischen User-ID fälschlich einen Namen einträgt.

Ein AD-Nutzereintrag enthält somit eine lange Liste teils optionaler, teils erforderlicher Attribute, die Windows benötigt. Jedem Nutzer ist beispielsweise ein Kontoname und ein SID (Security Identifier) zugeordnet. Es fehlen Attribute wie User- oder Gruppen-ID, die für ein Windows-System keinen Sinn ergeben, unter Unix jedoch zwingend erforderlich sind. Um AD für die Verwaltung von Unix-Clients fit zu machen, muss ein Administrator deshalb zunächst eine sogenannte Schemaerweiterung einspielen, sodass das Verzeichnis die Unix-spezifischen Attribute prinzipiell kennt. Eine Ausnahme bilden Windows Server ab 2003 R2, die per Default ein passendes Schema fest integriert haben. In der grafischen Nutzerverwaltung tauchen die zugehörigen Attribute jedoch erst auf, sobald der Administrator das „Identity Management for Unix“ nachinstalliert. Anschließend kann er die neuen Attribute für jeden Unix-Nutzereintrag tatsächlich mit Werten füllen.

POSIX-Attribute gemäß RFC 2307

Welche Attribute ein LDAP-Verzeichnis zur Speicherung Unix-spezifischer Informationen bereitstellen muss, regelt RFC 2307 („An Approach for Using LDAP as a Network Information Service“, [d]). AD hält sich zwar nur zum Teil an diesen Standard, doch das ist von untergeordneter Bedeutung. In erster Linie müssen sich LDAP-Client und -Server über das verwendete Format einig sein. Für die Benutzerverwaltung von Unix-Rechnern heißt der Client in

iX-TRACT

- Für den Umzug von Unix-Benutzerdaten in ein LDAP-Verzeichnis legt RFC 2307 fest, wie man die unterschiedlichen Attribute in Einklang bringen kann.
- Über die SASL-Bibliothek und das AD-interne Kerberos lässt sich die Kommunikation zwischen Clients und Domänen-Controller komfortabel sichern.
- Eine erfolgreiche Migration der Daten bietet nicht nur eine zentrale User-Verwaltung, man kann auch das unter Sicherheitsaspekten bedenkliche NIS abschalten.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

diesem Fall *nss_ldap*. Dabei handelt es sich um ein Modul für den Name Service Switch (NSS), ein flexibel erweiterbares System zur Anbindung von Unix an verschiedene Namensdienste. Lediglich AIX tanzt etwas aus der Reihe und verwendet statt NSS ein eigenes Modulsystem namens LAM, das sich jedoch auf ganz ähnliche Weise an AD anbinden lässt [c]. Beide Implementierungen greifen per LDAP auf die X.500-Objekte im AD zu. Dazu aktiviert der Administrator das LDAP-Modul in */etc/nsswitch.conf* und legt in einer weiteren Konfigurationsdatei fest, welche LDAP-Anfragen es an den Server stellen und wie es die Ergebnisse interpretieren soll. Je nach Distribution heißt die Konfigurationsdatei für das NSS-Modul */etc/ldap.conf* oder */etc/libnss-ldap.conf*. Sie ist nicht zu verwechseln mit der Datei */etc/openldap/ldap.conf*, die systemweite Voreinstellungen für die OpenLDAP-Kommandozeilenprogramme und ähnliche Werkzeuge enthält.

Als Standard erwartet *nss_ldap* die sogenannten POSIX-Attribute für Benutzer- und Systemdaten wahlweise in einem durch RFC 2307 festgelegten Schema oder gemäß des Vorschlags RFC 2307bis mit geänderter Definition für Benutzergruppen. Wer ein Schema mit anderen Attributnamen verwendet, kann sie mit dem Kommando *map* in der Konfigurationsdatei des *nss_ldap*-Moduls auf die RFC-Namen abbilden. Ältere AD-Installationen verwenden zum Speichern der POSIX-Attribute häufig die Schemaerweiterung aus den Services for Unix 3.x (SfU). Hier sind einige Mappings nötig, bis Unix die Einträge auch verwenden kann. Seit Windows Server 2003 R2 liefert Microsoft ein neues Schema für die POSIX-Attribute mit, das sich weitgehend mit RFC 2307 deckt. Schemaerweiterungen lassen sich allerdings nicht einfach rückgängig machen: Wer schon die SfU-Erweiterungen für die POSIX-Attribute eingespielt hat, muss beim Umstieg auf 2003 R2 an dieser Stelle mit Schwierigkeiten rechnen. Auch wenn der DC noch unter einer älteren Windows-Version läuft, sollte man deshalb bei einer nötigen Schemaerweiterung nicht mehr eines der SfU-Schemata, sondern die R2-Version verwenden.

Nicht nur technische Aspekte zählen

Nachdem das AD prinzipiell dafür gerüstet ist, alle benötigten Daten für Unix-Nutzer zu speichern, bleibt noch zu klären, wie die Daten letztendlich aus bestehenden NIS-Maps in den neuen Verzeichnisdienst gelangen. Das grafische Verwaltungsprogramm „Active Directory Users and Computers“ ist prinzipiell ein möglicher Weg, POSIX-Attribute einzelner Benutzer manuell nachzutragen – sofern das Subsystem „Identity Management for Unix“ auf dem DC nachinstalliert ist. Muss man umfangreichere Datenbestände migrieren, ist Automatisierung Pflicht. Da AD eine standardkonforme LDAP-Schnittstelle zur Verfügung stellt, kann ein Administrator dazu auf herstellerunabhängige Werkzeuge zurückgreifen. Bestes Beispiel sind die PADL-Migrations-Tools [a], ein frei verfügbarer Satz von Perl-Skripten zur Übernahme von NIS-Daten in ein LDAP-Verzeichnis. Jedes Skript existiert in einer Online- und einer Offline-Variante. Die Offline-Skripte sind speziell für OpenLDAP-Server konzipiert, die Online-Versionen funktionieren auch mit AD. Administratoren mit einem Hang zum Eigenbau können sich mit den Standardkommandos *ldapadd* und *ldapmodify* eigene Migrationsskripte basteln.

Wichtiger als die technischen Hürden sind an dieser Stelle ohnehin häufig die organisatorischen Fragen: Soll jeder Benutzer aus dem NIS ins AD übernommen werden oder nutzt man die Migration zur Konsolidierung des Gesamtbestands an Nutzerdaten? Sollen sämtliche AD-Nutzerkonten POSIX-Attribute erhalten oder genügt es, wenn sich nur ein Teil der Benutzer auch an Unix-Rechnern einloggen kann? Und welche Verfahrensregeln sollen bei der Zusammenführung mehrerer NIS-Domänen bei doppelt vergebenen Benutzernamen gelten? Im Beispiel-Migrationsprojekt bei NiS-AD sind die Rahmenbedingungen übersichtlich: Da die Administratoren seit Abschluss der ersten Projektphase AD zur Authentisierung an den Unix-Maschinen nutzen, besitzt jeder Anwender schon ein Konto mit eindeutigem Benutzernamen. Daher genügt es hier, anhand der Informationen aus den NIS-Maps lediglich die POSIX-Attribute nachzutragen.

Bei der NiS-AD laufen die DC unter Windows Server 2003 R2 und verwenden die mitgelieferte Schemaerweiterung für die POSIX-Attribute. Damit steht schon weitgehend fest, welches Feld aus der *passwd*-Map auf welches Attribut im AD abzubilden ist, die Tabelle „POSIX-Attribute“ verschafft einen Überblick. Wählen muss der Administrator bei den Attributen für den Benutzernamen und das Gecos-Feld. Standardmäßig pflegt AD bereits mehrere Attribute, die sich prinzipiell als Benutzername anbieten. RFC 2307 sieht dafür *uid* vor. Das gleichnamige AD-Attribut enthält jedoch einen Namen, der nicht als Kerberos-Principal bekannt ist. Wer sich in der Kerberos-Client-Konfiguration ein zusätzliches Mapping von Benutzer- auf Principal-Namen sparen möchte, ist mit dem Attribut *sAMAccountName* besser bedient. *userPrincipalName* als Alternative enthält zusätzlich den Realm-Anteil und überschreitet dadurch die Grenze von acht Zeichen für den Benutzernamen. Manche kommerziellen Unixe haben damit Schwierigkeiten, und auch auf aktuellen Linux-Systemen entsteht zumindest Verwirrung, wenn manche Standardwerkzeuge statt überlanger Benutzernamen nur die numerische User-ID anzeigen.

POSIX-Attribute

passwd-Feld	RFC-2307-Attribut	passende W2K3R2-Attribute	Bemerkung
username	*uid*	*uid*	nicht als Kerberos-Principal bekannt
		sAMAccountName	empfohlen
		userPrincipalName	Name länger als acht Zeichen
uid	*uidNumber*	*uidNumber*	
gid	*gidNumber*	*gidNumber*	
gecos	*gecos*	*gecos*	nicht über Administrations-GUI verfügbar
		description	empfohlen
		displayName	
		name	in Administrations-GUI: *Full Name*
		cn	in Administrations-GUI: *Full Name*
home	*homeDirectory*	*unixHomeDirectory*	
shell	*loginShell*	*loginShell*	

Für die Umsetzung der Felder aus der NIS-Map *passwd* auf POSIX-Attribute im LDAP legt RFC 2307 eine eindeutige Zuordnung fest. Ein AD mit dem R2-Schema des Windows Server 2003 lässt dem Administrator an manchen Stellen etwas Wahlfreiheit.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Auch für das *Gecos*-Feld der *passwd*-Map kennt AD das in RFC 2307 empfohlene Attribut *gecos* – allerdings nur bei direkten Anfragen an den Verzeichnisdienst. Das grafische Administrationswerkzeug „Active Directory Users and Computers“ zeigt das Feld nicht an. Besser eignet sich daher das Attribut *description*. Wer in der *Gecos*-Ausgabe lediglich den vollen Namen des Benutzers anzeigen möchte, kann auch auf die Standardattribute *displayName*, *name* oder *cn* ausweichen. Die beiden letztgenannten zeigt das Administrations-GUI im Feld *Full Name* an. Besonders einfach lässt sich das Passwort-Feld übertragen: Seit Einführung der kerberisierten Systemanmeldung in Projektphase eins wird es überhaupt nicht mehr benutzt, man sollte es daher ignorieren.

Sonderfall Gruppenzugehörigkeit

Schwieriger ist die Entscheidung, auf welche Weise AD den Inhalt der NIS-Map *group* abbilden soll. RFC 2307 sieht das Attribut *memberUid* vor. Es verwaltet für jede Unix-Gruppe eine Liste numerischer User-IDs ihrer Mitglieder, analog zur bisherigen NIS-Map. Allerdings stellt die grafische AD-Benutzerverwaltung auch dieses Feld standardmäßig nicht dar. Schlimmer noch: Da numerische User-IDs in der Windows-Welt keine Bedeutung besitzen, pflegt AD das Attribut nicht automatisch mit, wenn ein Administrator Gruppenmitgliedschaften verändert. Gleichnamige Gruppen können so unter Windows und Unix unterschiedliche Nutzergruppen umfassen. Systemübergreifende einheitliche Benutzerverwaltung sieht anders aus. Der Entwurf RFC 2307bis sieht deshalb vor, die Unix-Gruppenmitgliedschaften im Attribut *uniqueMember* abzubilden. Statt einer Liste von Unix-Benutzernamen enthält es schlicht Verweise auf die jeweiligen Benutzerobjekte im Verzeichnisdienst und entspricht damit dem Standardfeld *member*, das im AD auch die Gruppenzugehörigkeit für Windows-Systeme regelt. Falls alle Unix-Clients mit einem Gruppenschema nach RFC 2307bis umgehen können, bietet es sich an, den bequemen Weg zu wählen.

Nachdem sich die Administratoren darauf geeinigt haben, welche AD-Attribute sie für die Unix-Benutzerverwaltung benutzen wollen, müssen sie diese für Suchanfragen optimieren. Für besonders häufig abgefragte Attribute wie *uidNumber* sollte AD unbedingt einen Index anlegen. Sonst drohen erhebliche Performancenachteile. Die folgende Tabelle zeigt, welche sich dafür anbieten:

Attribut	Index?
GidNumber	ja
UidNumber	ja
Member	ja
LoginShell	nicht zwingend
UnixHomeDirectory	nicht zwingend

Umzug zunächst mit Haken

Nach all den Vorarbeiten haben die Unix-Administratoren bei NiS-AD nun das nötige Rüstzeug beisammen, das einerseits Migrationsskripte anpasst, die die Nutzerdaten aus den NIS-Maps ins AD übertragen und andererseits auf allen Clients das Modul *nss_ldap* so konfiguriert, dass es die Benutzerinformationen im AD erfragen und zurück in Unix-Sprache übersetzen kann. Listing 1 zeigt eine minimale Version der Konfigurationsdatei *ldap.conf* für das NSS-Modul.

Letzteres erwartet POSIX-Attribute unter den in RFC 2307 empfohlenen Namen. Über *map*-Anweisungen lassen sie sich auf Bezeichnungen abbilden, wie sie AD in Windows Server 2003 R2 benutzt. Die Verwendung des ungültigen Attributs *noSuchAttribute* deaktiviert praktisch die unerwünschten Attribute *memberUid* und *userPassword*. Das vermeidet Verwirrung und Fehler durch ungewollte Abfragen. Zusätzlich zu den schon erwähnten Mappings für Attribute übersetzt das Modul die Namen einzelner Objektklassen von RFC-Syntax in die passenden AD-Pendants. Die letzten beiden Zeilen der Beispielkonfiguration sind vor allem in größeren Umgebungen von Bedeutung.

Damit einzelne LDAP-Anfragen den DC nicht überlasten, liefert AD in den Voreinstellungen pro Anfrage maximal 1000 Objekte zurück. Übersteigt die Zahl der eingetragenen Nutzer diese Grenze, zeigt beispielsweise das Kommando *getent passwd* unter Linux deshalb nicht mehr die komplette Liste der Benutzerkonten an. Einzeln ist jedes der Konten jedoch sichtbar. Weitere Tücken drohen, wenn auch Gruppenmitgliedschaften die Tausender-Marke übersteigen. Über die Optionen *pagesize* und *nss_paged_results* erkennt *nss_ldap* die unvollständigen Serverantworten und stellt selbstständig weitere Anfragen nach den noch fehlenden Informationen. *getent passwd* funktioniert dann auch in größeren Umgebungen ohne Überraschungen. Bleibt ein Haken: Damit die minimale Konfiguration tatsächlich funktioniert, mussten die Administratoren bei NiS-AD die Voreinstellungen des DC so ändern, dass er anonyme Abfragen der POSIX-Attribute erlaubt. Das beeinträchtigt die Vertraulichkeit der gespeicherten Daten und bereitet den Administratoren deshalb so manche Bauchschmerzen. Diese Schwachstelle wollen sie deshalb schnellstmöglich wieder loswerden.

Tutorialinhalt

Teil I: Migration der Authentifizierung

Teil II: AD-Benutzerinformationen für unixoide Systeme

Teil III: Linux-Dienste für SSO an AD anbinden und Erweiterung auf Active Directory Forest

Listing 1: Konfiguration */etc/ldap.conf*

```
base dc=nis-ad,dc=de
uri ldap://nis-ad.de
ldap_version 3
# Benutzerattribute
nss_map_attribute       uid             sAMAccountName
nss_map_attribute       homeDirectory   unixHomeDirectory
nss_map_attribute       gecos           description
# Gruppenattribut anhand RFC 2307bis
nss_map_attribute       uniqueMember    Member
# unbenutzte Attribute aus RFC 2307
nss_map_attribute       memberUid       noSuchAttribute
nss_map_attribute       userPassword    noSuchAttribute
# verwende Standardklassen User und Group in Active Directory
nss_map_objectclass     posixAccount    User
nss_map_objectclass     posixGroup      Group
nss_map_objectclass     shadowAccount   User
nss_map_attribute       objectClass     objectCategory
# stelle Mehrfachanfragen, falls ein Suchergebnis die serverseitige
# Maximalgröße übersteigt
pagesize                1000
nss_paged_results       yes
```

NiS-AD sagt NIS ade

Zuvor ist jedoch die Zeit gekommen, der Benutzerverwaltung im NIS endgültig den Garaus zu machen. Die Administratoren passen dazu die Konfigurationsdatei */etc/nsswitch.conf* an und ersetzen in den Zeilen für *passwd* und *group* den Eintrag *nis* durch *ldap*. Das Modul *nss_ldap* ist nun aktiv und greift auf die AD-Informationen zu. Wer sofort testen möchte, ob die LDAP-Anfragen tatsächlich wie gewünscht funktionieren, sollten via *nscd -i passwd* und *nscd -i group* eventuell lokal zwischengespeicherte Informationen verwerfen. Als Test bietet sich die Prüfung an, ob Standardkommandos wie *id*, *groups*, *ls -l* oder *finger* die erwarteten Nutzerdaten zurückliefern.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Das Ziel der einheitlichen Benutzerverwaltung im gesamten NiS-AD-Netz haben die Administratoren damit erreicht. In puncto Sicherheit haben sie durch die Umstellung auf LDAP statt NIS bislang jedoch kaum hinzugewonnen: Wie erwähnt schickt in der aktuellen Konfiguration jeder Clientrechner seine Anfragen anonym zum DC, die Antworten erhält er weder verschlüsselt noch digital signiert. Angreifer können sich nach wie vor durch gefälschte Serverantworten unberechtigten Zugang zu einem System verschaffen. Auch wenn das Belauschen des Netzverkehrs zwischen Client und DC seit der Umstellung auf Kerberos keine Passwörter mehr preisgibt, erlaubt es doch beispielsweise Rückschlüsse auf das Nutzerverhalten. Außerdem wollen die Administratoren möglichst rasch ihre Bauchschmerzen vertreiben, indem sie den anonymen Zugriff auf die POSIX-Attribute wieder unterbinden.

Heilung verspricht die SASL-Bibliothek (Simple Authentication and Security Layer), mit deren Hilfe sich die LDAP-Verbindungen zwischen Client und DC per Kerberos schützen lassen. Dazu genügt es, auf jedem Unix-Client das Kerberos/GSSAPI-Modul für SASL nachzuinstallieren und in der Konfigurationsdatei der *nss_ldap* die SASL-Unterstützung zu aktivieren. Die passende Anweisung lautet schlicht *use_sasl on*. Das Kerberos-Protokoll gewährleistet automatisch Authentizität, Integrität und Vertraulichkeit der Kommunikation zwischen DC und Client – vorausgesetzt, das Modul *nss_ldap* kann für seine Anfragen auf ein gültiges Kerberos-Ticket zugreifen. In der aktuellen Umgebung ist das bei NiS-AD automatisch der Fall, sobald gewöhnliche Benutzer sich kerberisiert am System anmelden. Schwierigkeiten treten auf, wenn ein Benutzer länger angemeldet bleibt als seine Tickets gültig sind. Darüber hinaus verwenden *root* oder Systemdienste lokale Benutzerkonten, denen normalerweise kein Kerberos-Ticket zur Verfügung steht. Damit auch sie Nutzerdaten abfragen können, müssen die Administratoren doch noch ein wenig mehr Aufwand treiben.

Onlinequellen

[a] PADL Migrationstools
www.padl.com/OSS/MigrationTools.html

[b] *kstart*
www.eyrie.org/~eagle/software/kstart/

[c] LAM
www.redbooks.ibm.com/redbooks/pdfs/sg247165.pdf

[d] RFC2307
www.ietf.org/rfc/rfc2307.txt

[e] *iX*-Listing-Service
ftp.heise.de/pub/ix/ix_listings/

Vom Umgang mit den Tickets

Statt sämtliche Anwender im System stets mit gültigen Tickets zu versorgen, nutzen sie aus, dass die fundamentale Glibc-Bibliothek des Linux-Systems alle Anfragen nach Nutzerdaten – sofern vorhanden – über den *nscd*-Daemon kanalisiert. Stellen die Administratoren sicher, dass auf jedem Unix-Client ein *nscd* läuft und auf ein gültiges Ticket zugreifen kann, funktionieren die Abfragen von Benutzerinformationen auch ohne eigenes Kerberos-Ticket des aufrufenden Prozesses. Zwei Dinge sind dazu notwendig: Zum einen ein Daemon oder Cronjob, der regelmäßig ein aktuelles Ticket für den *nscd* besorgt und in einem sogenannten Credential Cache ablegt. Zum anderen müssen die Administratoren die Lage des Credential Cache in die Konfigurationsdatei des Moduls *nss_ldap* eintragen.

Für welchen Kerberos-Principal sie die Tickets anfordern, ist dabei nicht ausschlaggebend, solange im AD alle nötigen Zugriffsberechtigungen vorhanden sind. Da jeder Rechner über ein eigenes Maschinenkonto verfügt, bietet es sich an, den zugehörigen Principal auch für den *nscd* zu verwenden. Die nötigen Änderungen an der *nss_ldap*-Konfiguration in */etc/ldap.conf*, die die Kommunikation mit dem DC über das Kerberos-Plug-in der SASL-Bibliothek absichern, sind kurz:

```
use_sasl    on
krb5_ccname    FILE:/var/cache/nscd/krb5cc
```

Ein simpler Cronjob kümmert sich darum. dass der *nscd* immer auf ein aktuelles Kerberos-Ticket zurückgreifen kann. Die Option *-k* bewirkt, dass *kinit* kein Passwort, sondern eine Keytab erwartet. Das Ticket stellt der DC auf das Maschinenkonto des jeweiligen Clientrechners aus. Der Eintrag des zugehörigen Principals erfolgte in der ersten Projektstufe [1] beim Erzeugen der Host-Keytab mit *ktutil*. Die Gültigkeitsdauer der Tickets bestimmt die Frequenz des Cronjobs.

```
#!/bin/sh
PRINCIPAL=`hostname -s`
kinit -k -c FILE:/var/cache/nscd/krb5cc ⏎
                                "$PRINCIPAL"
```

Statt des Cronjobs ließe sich mit passender Konfiguration beispielsweise auch das Hilfsprogramm *kstart* [b] verwenden. In jedem Fall funktionieren die Anfragen nun auch mit DCs, die – wie bei AD üblich – keine anonymen Abfragen erlauben.

Zweiter Teilschritt abgeschlossen

Damit haben die Administratoren bei NiS-AD das Ziel der Phase zwei ihres Migrationsprojektes erreicht. Die gesamte Benutzerverwaltung für Windows- wie Unix-Rechner läuft zentral über das AD. Weder Passwort- noch Nutzerdaten lassen sich über das Netz ausspähen, und auch gegen gefälschte Serverantworten setzen sich die Clients inzwischen mit kryptografischen Methoden zur Wehr. Damit ist das Pflichtprogramm abgearbeitet. In der im dritten und letzten Teil dieses Tutorials vorgestellten Phase drei des Projektes folgt die Kür: Die Administratoren wollen die Single-Sign-On-Fähigkeiten von AD ausnutzen. Einige weitere Unix-Netzdienste, die den Nutzer bislang noch nach einem eigenen Passwort fragen, binden sie so ins System ein, dass ein Kerberos-Ticket als Identitätsnachweis ausreicht. Ist auch Phase drei beendet, gehören lästige Passwortabfragen an Mail- oder Webserver der Vergangenheit an. Darüber hinaus erweitern die Administratoren die vorgestellten Konzepte auf einen sogenannten Active Directory Forest, der mehrere getrennte Domänen umfasst.

(avr)

MARK PRÖHL UND MICHAEL WEISER

arbeiten bei der science + computing ag und sind als Consultants in den Bereichen Kerberos, LDAP und AD-Integration aktiv. Seit mehreren Jahren leiten Sie auch Trainingsveranstaltungen zu diesen Themen.

Literatur

[1] Mark Pröhl, Michael Weiser; AD-Integration; Diener zweier Herren; Tutorial: Active Directory auch für Unix und Linux; *iX* 10/2008, S. 134





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Variables Greylisting zur Spam-Abwehr



Schwarz-Weiß-Mailerei

Marcel Lohmann

Greylisting gilt als probates Mittel gegen E-Mail-Spam. Die Verursacher treffen jedoch bereits Vorkehrungen dagegen. Darüber hinaus hat es konzeptbedingte Schwächen. Beidem können Mailserver-Betreiber durch ein erweiterbares, variables Greylisting begegnen.

Wer als Postmaster mit Massen von Spam zu kämpfen hat, zieht früher oder später den Einsatz von Greylisting in Betracht. Nur so kann man die Massen von Zustellversuchen aus Bot-Netzen in den Griff bekommen, da viele Quell-IP-Adressen nicht in Blacklists auftauchen. Es wäre auch nicht ratsam, alle dynamisch vergebenen IP-Adressen generell vom Mailversand auszuschließen und somit unter Generalverdacht zu stellen.

Unter Mail-Administratoren gibt es berechtigte Bedenken gegenüber Greylisting, da das Konzept einige Schwächen aufweist. Erst einmal steht jeder einliefernde Mailserver unter dem Verdacht, Spam abzuliefern und unterliegt dem Greylisting – auch legitime Mailserver von großen ISPs. Der größte Nachteil besteht aber darin, dass Greylisting den Mailtransport bremst, da es den jeweils ersten Zustellversuch verhindert. Die Zeitspanne bis zum zweiten Zustellversuch legt allein der sendende Server fest, sie kann zwischen wenigen Sekunden und mehreren Stunden liegen. Wie sich diese Schwächen auf ein Minimum reduzieren lassen, soll das Folgende erläutern.

Das Whitepaper vom Greylisting-Erfinder Evan Harris definiert, dass ein Tripel aus IP des Senders, der Absenderadresse und der Empfängeradresse bestimmte Phasen durchläuft [1]. Außerdem erläutert es drei unterschiedliche Fristen, die sendende Mailserver einhalten müssen, damit sie eine Mail – definiert durch besagtes Tripel – zustellen können. Frühestens nach der Verzögerungszeit werden weitere Zustellversuche akzeptiert – bis zur Verfallszeit; danach scheitern erneute Zustellversuche. Erfolgt eine Einlieferung im Zeitraum dazwischen, passieren alle weiteren Mails, die das Tripel beschreibt, den Mailserver. Auch die Tripel unterliegen einer dritten Frist – der Ablaufzeit. Erfolgt vor der Ablaufzeit kein erneuter Zustellversuch, so gilt die Kommunikation als veraltet und die Datenbank verwirft das Tripel. Alle Fristen lassen sich durch weitere Zustellversuche aufschieben.

Harris empfiehlt eine Stunde Verzögerungszeit, vier Stunden Verfallszeit und 36 Tage Ablaufzeit. Andere Quellen empfehlen abweichende Zeiten, und Standard-Greylisting-Programme können die Fristen variabel halten. Doch welche Fristen sind richtig? Kann man die Verzögerungszeit auf fünf Minuten reduzieren, ohne Spammern – die sich allmählich auf Greylisting einstellen –

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Tür und Tor zu öffnen? Sind 20 Minuten ein guter Mittelwert? Die Lösung liegt gerade in einer flexiblen Gestaltung dieser Frist, denn das Optimum hängt von mehreren Faktoren ab, die sich nicht auf drei Zahlenwerte reduzieren lassen.

Es muss also ein Greylisting-Algorithmus her, der die Fristen dynamisch berechnet und dazu die gegebenen Faktoren berücksichtigt. Eine Implementierung in Java als Policy Service für Postfix soll im Folgenden als Beispiel dienen [2]. Das Installieren des *JGreylister* genannten Programms beschreibt die Anleitung im Installations-Paket. Die Konfiguration entspricht im Auslieferungszustand den Empfehlungen von Evan Harris, aber sie lassen sich variieren und an die jeweiligen Bedingungen anpassen.

Eclipse macht's einfach

Am einfachsten lassen sich Anpassungen mit Eclipse vornehmen. Dazu legt man ein neues Java-Projekt an und fügt zum Build-Path die externe Jar-Datei *jgreylister.jar* aus dem Installationspaket hinzu. Java-konform sollte man anschließend ein Package mit dem eigenen Domain-Namen anlegen, beispielsweise org.example.rules. Dorthin gehören alle weiteren Klassen, die die Regeln für das Greylisting bestimmen.

Die erste Kategorie von Klassen legt die Verzögerungszeit fest, die ein Tupel auferlegt bekommt. Allgemein „Tupel" deswegen, da zu den Werten des Tripels Informationen wie Hostname des Absenders, Domain-Anteil der Absenderadresse und die HELO/EHLO-Angabe zur weiteren Auswertung hinzukommen. Der Programmcode aus Listing 1 beschreibt eine Klasse *HostNotGivenRule*, die das Interface *DelayRule* implementiert. Die Methode *getDelayTime()* dient zur Bestimmung der Verzögerungszeit bei der ersten Sichtung des Tupels. Das Tupel wird über das Objekt *SMTPInformation* an die Methode als Grundlage für die Berechnung übergeben. Neben der IP-Adresse, dem Absender und dem Empfänger enthält die Klasse unter anderem den rückwärts aufgelösten Hostnamen und den HELO/EHLO-String aus dem SMTP-Dialog. Falls in diesem Beispiel der Hostname nicht rückwärts auflösbar sein sollte („unknown"), gilt eine Verzögerungszeit von zehn Minuten. In allen anderen Fällen gibt es keine Verzögerungszeit; ein zweiter Einlieferungsversuch wäre also sofort erlaubt.

Weitere Bedingungen ließen sich in dieser Methode unterbringen, was unweigerlich zu einem unübersichtlichen *if-then-else*-Konstrukt führen würde. Die schönere und wartbarere Variante ist allerdings, für jede Bedingung eine eigene Klasse zu schreiben und jede Bedingung in einer eigenen Methode *getDelayTime()* unterzubringen. Alle Klassen bilden eine Regelkette, die gemeinsam eine Gesamtverzögerung ergibt. Die Verzögerungszeit lässt sich durch eine Regel nicht nur verlängern, sondern auch verkürzen, indem die Methode einfach eine negative Anzahl von Minuten zurückgibt. So kann man etwa auch Mailserver belohnen, deren Hostnamen plausibel erscheinen, also zum Beispiel mit „mail" oder „smtp" beginnen (Listing 2).

Das Interface *DelayRule* verlangt *getDelayTimeWithHistory()*, die zum Einsatz kommt, wenn das Tupel bereits aktenkundig ist (über die Klasse *MailHistory*). Die Historie umfasst die Anzahl der Sekunden seit der ersten Sichtung, die Sekunden bis zum Erreichen der (beim letzten Mal errechneten) Verzögerungszeit und die Anzahl der bisherigen fehlgeschlagenen Einlieferungsversuche. Listings 1 und 2 ignorieren die Historie geflissentlich, aber Listing 3 zeigt, wie sich wild gewordene Mailserver in die Schranken weisen lassen.

Welche Java-Methoden welche Berechnungen anstellen, ist dem Program-

iX-TRACT

- Greylisting gilt nach wie vor als probates Mittel zur Abwehr unerwünschter E-Mails, auch wenn die Spam-Versender bereits Gegenmaßnahmen ergreifen.
- Mit einer abgestuften Strategie, die unter anderem eine Whitelist legitimer Absender umfasst, lassen sich die oftmals kritisierten Nebenwirkungen des Greylisting in praktikablen Grenzen halten.
- Eine Umsetzung sinnvoller Greylisting-Policies für Postfix unter Java namens JGreylister steht auf dem *iX*-Listing-Service (ftp.ix.de) zur Verfügung.

Listing 1

```
package com.example.rules;

import de.malowa.greylister.MailHistory;
import de.malowa.greylister.SMTPInformation;
import de.malowa.rules.delay.DelayRule;

public class HostNotGivenRule implements DelayRule {

    public int getDelayTime(SMTPInformation mail) {
        if (mail.getClientHost().equals("unknown"))
            return 10;
        return 0;
    }

    public int getDelayTimeWithHistory(SMTPInformation info,
                                       MailHistory history) {
        return getDelayTime(info);
    }

    public void update() {
        // Do nothing
    }
}
```

Clients ohne Pointer Record (auch Reverse DNS genannt) erhalten eine Zeitstrafe.

Listing 2

```
package com.example.rules;

import de.malowa.greylister.MailHistory;
import de.malowa.greylister.SMTPInformation;
import de.malowa.rules.delay.DelayRule;

public class PossibleMTARule implements DelayRule {

    public int getDelayTime(SMTPInformation mail) {
        if (mail.getClientHost().startsWith("mail.")
                || mail.getClientHost().startsWith("smtp."))
            return -5;
        return 0;
    }

    public int getDelayTimeWithHistory(SMTPInformation info,
                                       MailHistory history) {
        return getDelayTime(info);
    }

    public void update() {
        // Do nothing
    }
}
```

Clients mit für reguläre MTAs typischen Namen erhalten eine Belohnung.

Listing 3

```
package com.example.rules;

import de.malowa.greylister.MailHistory;
import de.malowa.greylister.SMTPInformation;
import de.malowa.rules.delay.DelayRule;

public class AggressiveHostRule implements DelayRule {

    public int getDelayTime(SMTPInformation info) {
        return 0;
    }

    public int getDelayTimeWithHistory(SMTPInformation info,
                                       MailHistory history) {
        if (history.getPassedSeconds() < 120 &&
                          history.getBlockedmailcount() > 3)
            return 90;
        return 0;
    }

    public void update() {
        // do nothing
    }

}
```

Ständig wiederkehrende Clients bekommen eine zusätzliche Zeitstrafe verpasst.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

mierer vollkommen freigestellt. So sind auch tageszeitabhängige, durch reguläre Ausdrücke definierte oder durch Properties konfigurierbare Regeln denkbar. Letztere erfordern das regelmäßige Neueinlesen der Properties. Die Methode *update()* des Interface ist genau dafür gedacht und soll in einer der nächsten Versionen diese Updates anstoßen. In Attributen der Klasse kann man die variablen Daten zwischenspeichern. Da die Regeln nur ein einziges Mal im Programm instanziiert sind und für jedes Tupel gelten, ist es also nicht ratsam, in einem Attribut der Klasse Informationen abzulegen, die sich auf ein Tupel beziehen.

Nun existiert eine Reihe von Regeln, die dem Programm bekannt sein müssen, damit es sie verwendet. Dazu ist es notwendig, die von Eclipse im Hintergrund erzeugten Binärdaten aus dem *bin*-Ordner des Projekts in den *ext*-Unterordner der *jgreylister*-Installation zu kopieren. Die Unterverzeichnisse sind unbedingt beizubehalten, also aus *bin\org\example\rules\AggressiveHostRule.class* wird *ext/org/example/rules/AggressiveHostRule.class*. Nach dem Kopieren ist die Datei *conf/rules.properties* im Installationsverzeichnis anzupassen; sie enthält dann die neuen Regeln (Listing 4 zeigt, wie man die drei bisher definierten Regeln zu der Standardregel hinzufügt).

Listing 4

```
delay = com.example.rules.HostNotGivenRule,\
  com.example.rules.PossibleMTARule ,\
  com.example.rules.AggressiveHostRule
cleanup = com.example.rules.ManyNumbersRule,\
  com.example.rules.DynamicIPRule
white = com.example.rules.AbuseRule,\
  com.example.rules.AcceptMTARule
pass = com.example.rules.InsaneMailserverRule
black = com.example.rules.BadCoconutRule
```

In der Datei *rules.properties* eingetragene Regeln bilden zusammen mit Standardregeln ein komplexes Regelwerk.

Listing 5

```
package com.example.rules;

import java.util.Calendar;
import java.util.Date;
import java.util.GregorianCalendar;

import de.malowa.greylister.MailHistory;
import de.malowa.greylister.SMTPInformation;
import de.malowa.rules.cleanup.CleanUpRule;

public class ManyNumbersRule implements CleanUpRule {

     public Date dateToRemoveNoRetry(SMTPInformation info,
                                             MailHistory history) {
          if (info.getClientHost().matches(".*(\\d{1}\\D*){5,}")) {
               GregorianCalendar cal = new GregorianCalendar();
               cal.add(Calendar.HOUR_OF_DAY, 1);
               return cal.getTime();
          }
          return null;
     }

     public Date dateToRemovePassedEntry(SMTPInformation info,
               MailHistory history) {
          return null;
     }

}
```

Hosts mit vielen Ziffern melden sich selten ein weiteres Mal. Sie können schneller wieder aus der Datenbank entfallen.

Wiederkehrende Aufräumarbeiten

Mit jeder eintreffenden Mail wächst die Datenbank, was deren Performance beeinträchtigt. Viele Datensätze sind aber nach einiger Zeit obsolet, zum Beispiel die Tupel, deren Ablaufzeit oder Verfallszeit in der Vergangenheit liegt. Das Programm entfernt automatisch solche veralteten Einträge.

Dazu muss es Regeln für die Bestimmung der Ablaufzeit und der Verfallszeit geben, die sich dynamisch aus der SMTP-Information und der Historie berechnen lassen. Anders als bei der Bestimmung der Verzögerungszeit können die Regeln aber nicht durch einfaches Summieren der Zeiten eine Ablaufzeit bestimmen. Wenn eine Regel greift, bestimmt sie allein die Ablauf- oder Verfallszeit.

Das dafür vorgesehene Interface in Java lautet *CleanupRule* und man kann mit der Methode *dateToRemoveNoRetry()* die Ablaufzeit bestimmen. Die Methode *dateToRemovePassedEntry()* bestimmt dagegen die Verfallszeit. Wenn die Aufräumregel keine Zeit bestimmen kann oder will, muss die Methode *NULL* zurückliefern; in dem Fall gilt die nächste Regel. Erst wenn die Regelkette komplett durchlaufen und die Zeit immer noch unbestimmt ist, greift automatisch eine Standardregel, die die Ablaufzeit auf vier Stunden in die Zukunft und die Verfallszeit auf 36 Tage in die Zukunft setzt.

Auf diesem Wissen basiert nun eine Regel, die die Ablaufzeit reduziert, wenn im Hostnamen mindestens fünf Zahlen vorhanden sind. Listing 5 zeigt, wie man die Ablaufzeit auf eine Stunde in die Zukunft setzt und die Verfallszeit unberührt lässt.

Nicht jeder nutzt die Smarthosts seines Providers: Es gibt auch Clients, die legitime Mails direkt über den DSL-Anschluss versenden. Das können IP-Kameras sein, die regelmäßig ihren Status per Mail kundtun, oder normale Mailprogramme. Wenn diese das Greylisting schaffen, ist es allerdings nicht notwendig, sie für 36 Tage in der Datenbank festzuhalten. Nach spätestens 24 Stunden erfolgt eine Zwangstrennung und die IP-Adressen in der Datenbank repräsentieren ganz andere Hosts. Listing 6 zeigt, wie sich zumindest diejenigen der großen deutschen DSL-Provider nach 24 Stunden aus der Datenbank tilgen lassen.

Diese beiden Regeln sind nach dem Kompilieren in das entsprechende Verzeichnis unter *ext/* zu kopieren. Die *conf/rules.properties* muss so editiert werden, dass die neuen Regeln auch gelten.

Ohne Weiß kein Grau

Ein ordentliches Greylisting kommt natürlich nicht ohne Fallunterscheidung aus. Generell steht prinzipbedingt zunächst jedes Tupel auf einer „Whitelist“, wenn es das Greylisting überwunden hat; jedenfalls so lange, bis der Datensatz nach der Ablaufzeit aus der Datenbank verschwindet. Außerdem gibt es Regeln, die greifen, bevor ein Tupel überhaupt das Greylisting durchläuft.

Das dazugehörige Interface heißt *WhitelistRule* und erfordert das Implementieren der Methode *shouldBeWhitelisted()*. Ein Anwendungsszenario wäre, alle Mails anzunehmen, die an „postmaster“ oder „abuse“ gehen sollen, denn Spammer verwenden diese Empfänger relativ selten für ihre Werbebotschaften. Das Listing 7 zeigt, wie man das Szenario umsetzen kann. Die erste Regel, die zutrifft, beendet die Abarbeitung der Regelkette von WhitelistRules.

Außer der regelbasierten Whitelist gibt es eine (noch) nicht konfigurierbare interne Whitelist, die sich automatisch durch eintreffende E-Mails erweitert. Wenn fünf verschiedene Empfänger-Absender-Kombinationen zu einer IP-Adresse das Greylisting überwunden haben, kommt sie auf die interne Whitelist. Jeglicher Mailverkehr von dort umgeht ab diesem Moment das Greylisting und wird automatisch akzeptiert.

Da sich diese Whitelist in der internen Datenbank befindet, lässt sie sich manuell füllen, etwa für nicht-RFC-konforme Mailserver. Die dafür notwendige Tabelle lautet *WHITEDOMAIN* und die Spalte für die IP-Adresse 1 *DOMAIN*. Als kleinen Bonus akzeptiert die Tabelle auch einen *DOMAIN*-Eintrag in

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

der Form 192.0.2, womit der Bereich 192.0.2.0/24 gemeint ist.

Statt nun alle größeren ISPs und Mailprovider in die Whitelist aufzunehmen, kann man sich die Arbeit auch abnehmen lassen und die Whitelist von dnswl.org nutzen, die sich praktisch wie jede DNSBL abfragen lässt. Nur dass eine IP-Adresse auf der Liste steht, wenn sie für einen SMTP-Client akzeptabel erscheint und Mails von dort eben nicht abgelehnt werden sollten. Leider unterstützt Postfix diese umgekehrte Logik nicht von Haus aus und erfordert einige Umwege. Da JGreylister ohnehin in Postfix eingebunden ist, kann die Abfrage der DNSWL auch aus dem Programm heraus erfolgen. Sobald in der Datei *conf/jgreylister.properties* der Parameter useDNSWL „true" lautet, passieren alle Mails von auf dnswl.org gelisteten IP-Adressen ungestört.

Wer weiß sagt ...

Wenn sich alle Clients an die bisher vorgegebenen Regeln halten würden, ergäbe sich ein angenehmes, sauberes Greylisting. Doch es wäre zugleich nutzlos: Es funktioniert ja gerade deswegen, weil eben nicht alle Clients die Regeln einhalten, vor allem nicht die von Spammern. Wie üblich birgt der Übergangsbereich die meisten Tücken: Viele legitime Clients stehen weder auf einer Whitelist noch halten sie sich hundertprozentig an die RFCs. Zu großzügige Whitelist-Regeln wären ein genereller Freifahrtschein für Spam. Für genau diesen Zweck gibt es „Gnadenregeln", die in

Listing 6

```
package com.example.rules;

import java.util.Calendar;
import java.util.Date;
import java.util.GregorianCalendar;

import de.malowa.greylister.MailHistory;
import de.malowa.greylister.SMTPInformation;
import de.malowa.rules.cleanup.CleanUpRule;

public class DynamicIPRule implements CleanUpRule {

    public Date dateToRemoveNoRetry
                (SMTPInformation info, MailHistory history) {
        return null;
    }

    public Date dateToRemovePassedEntry(SMTPInformation info,
            MailHistory history) {
        if (info.getClientHost().endsWith("dip0.t-ipconnect.de")
                || info.getClientHost().endsWith
                                    ("dip.t-dialin.net")
                || info.getClientHost().endsWith
                                   ("pools.arcor-ip.net")
                ||
info.getClientHost().endsWith("alicedsl.de")) {
            GregorianCalendar cal = new GregorianCalendar();
            cal.add(Calendar.DAY_OF_MONTH, 1);
            return cal.getTime();
        }
        return null;
    }

}
```

Dynamisch vergebene IP-Adressen müssen sich nicht länger als einen Tag in der Datenbank befinden. Dann nutzt bereits ein anderer Computer oder Router dieselbe Adresse.

Listing 7

```
package com.example.rules;

import de.malowa.greylister.SMTPInformation;
import de.malowa.rules.white.WhitelistRule;

public class AbuseRule implements WhitelistRule {

    public boolean shouldBeWhitelisted(SMTPInformation info) {
        if (info.getRecipient().startsWith("abuse@")
                || info.getRecipient().startsWith("postmaster@"))
            return true;
        return false;
    }

}
```

Freie Bahn für E-Mails an die wenig bespammten Postmaster- und Abuse-Accounts



© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Kraft treten, wenn ein Tupel bereits auf der Greylist steht und ein zweiter (oder weiterer) Zustellversuch stattfindet. In dem Fall kann man sich entscheiden, ob man diesen Zustellversuch zum Anlass nimmt, die Mail passieren zu lassen.

Das zu implementierende Interface *PassRule* setzt die Methode *shouldBe Whitelisted()* voraus. Listing 8 zeigt, wie man wahrscheinliche Mailserver akzeptiert, noch bevor die Verzögerungszeit abgelaufen ist. Wenn Spammer ihren Hostnamen mit „mail“ oder Ähnlichem beginnen lassen, müssen sie also mindestens einen zweiten Zustellversuch starten, damit Mails von dort unverzüglich durchkommen. Spammer tun das in der Regel nicht, legitime Server profitieren dagegen von dieser „Begnadigung“.

Ein weiteres Szenario für diese Sonderregel ist das Akzeptieren „wildgewordener“ Mailserver. Ab und zu kommt es vor, dass solche Server alle 30 Sekunden einen Zustellversuch unternehmen. Dabei ergibt sich natürlich eine immer wieder neu berechnete Verzögerungszeit, die in der Zukunft endet. Wenn man Pech hat, endet die Verzögerungszeit nie. In dem Fall ist eine Regel denkbar, die nach 30 Minuten und mindestens sechs Zustellversuchen die Mail akzeptiert.

Listing 8

```
package com.example.rules;

import de.malowa.greylister.MailHistory;
import de.malowa.greylister.SMTPInformation;
import de.malowa.rules.pass.PassRule;

public class AcceptMTARule implements PassRule {

    public boolean shouldBeWhitelisted
                  (SMTPInformation info, MailHistory history) {
        if (history.getBlockedmailcount() > 0)
            if (info.getClientHost().startsWith("mail")
                    || info.getClientHost().
                                    startsWith("smtp")
                    || info.getClientHost().
                                    startsWith("mo-p")
                    || info.getClientHost().
                                 matches("mx(\\d)*\\..*"))
                return true;
        return false;
    }

}
```

Wenn sie einen zweiten Versuch starten, werden offensichtlich legitime MTAs durchgewinkt.

... muss auch schwarz sagen

Regeln, die ausschließlich Mails akzeptieren, reichen nicht immer für ein komplettes Regelwerk. So gibt es nämlich auch immer wieder Spammer, die das Greylisting passieren, weil ihre Systeme sich wie „echte“ Mailserver verhalten. Immer wieder tauchen melanie@example.org und Kolleginnen auf, die von verschiedenen IP-Adressen aus die gleichen Nachrichten einliefern wollen. Glücklicherweise melden sie sich immer mit dem gleichen HELO-Eintrag, was das Ausfiltern recht einfach macht. Wie man solche Absender am geschicktesten aussperrt, zeigt Listing 9.

Dieser letzte Ausweg sollte möglichst sparsam dosiert sein, denn alle Zustellversuche führen zu einem harten 5xx-Fehler mit entsprechendem Hinweis. Eine so abweisende Behandlung haben ausschließlich Spammer verdient.

Mit ein wenig Analyse des eigenen Mailverkehrs lassen sich die möglichen Regeln zu einem wirksamen Greylisting-Bollwerk kombinieren. Spammer können es kaum überwinden, während legitimen Mailservern viel Freiraum bei der Mailzustellung bleibt. Damit die Gefahr von False Positives in Maßen bleibt, empfiehlt es sich, einen Mailklassifizierer wie *amavisd* zuzuschalten und lieber ein paar mehr Mails anzunehmen als eine zu viel abzulehnen.

Listing 9

```
package com.example.rules;

import de.malowa.greylister.SMTPInformation;
import de.malowa.rules.black.BlacklistRule;

public class BadCoconutRule implements BlacklistRule {

    public boolean shouldBeBlacklisted(SMTPInformation info) {
        if (info.getHelo().equals("mail.onlinemail.cc")
                  || info.getHelo().equals("mail.fivemail.cc")
                  || info.getHelo().equals("mail.mailview.cc")
                  || info.getHelo().equals("mail.spacemails.cc")
                  || info.getHelo().equals("mail.fishmail.cc")
                  || info.getHelo().equals("mail.mediamail.cc"))
            return true;
        return false;
    }
}
```

Penetrant spammende Server stoßen auf eine harte Abweisung.

Fazit

In der beschriebenen Konstellation läuft die Beispielimplementierung auf mehreren produktiven Systemen, mit einem an die dortige Situation angepassten und bei Bedarf erweiterten Funktionsumfang. Die genannten Regeln dienen im Artikel der Veranschaulichung und als Basis für eigene Ideen. In der konkreten Umsetzung erfahren grob zusammengefasst typische Kennzeichen von MTAs und Hostnamen in .de, .at und .ch eine Bevorzugung, während dynamisch vergebene IP-Adressen und Hostnamen aus Spammer-freundlichen Gegenden als Negativkriterien gelten.

Die Einführung des Greylisting-Verfahrens hat das Spam-Aufkommen auf dem Hauptsystem gewaltig reduziert und zu sehr positiven Reaktionen der Anwender geführt. Zwischen 7000 und 10 000 Mails landen täglich nicht in irgendwelchen Spam-Ordnern, weil der Mailserver sie gar nicht erst annimmt. Es stehen immer zwischen 190 und 250 Einträge auf der Greylist, und so müssen nur etwa fünf Mails am Tag das Greylisting neu passieren, da die IP-Adressen der Absender vorher nicht in Erscheinung getreten sind. Nur bei diesen ist die oft verschriene verzögerte Zustellung zu verzeichnen. Die Wartezeit liegt bei durchschnittlich 20 Minuten und ist eher vom Verhalten des Absender-Mailservers abhängig als von der auferlegten Verzögerungszeit.

Alle anderen monatlich 1900 legitimen Mails werden durch die Whitelists akzeptiert, von denen der nachgeschaltete Amavis allerdings 150 als Spam markiert. Nur sind 150 Spams deutlich weniger als die ungefähr 230 000, die Amavis mit Spamassassin sonst zu bewältigen hätte, was eine Menge Rechenzeit einspart. Auf jeden Fall spart es die langwierige Suche nach False Positives in einer solchen Masse von Mails.

Durch stichprobenartige Analysen der Log-Dateien und Hinweise von Kunden gibt es eine Rate von etwa einem False Positive pro Monat. Diese ergeben sich ausschließlich durch Server, die nie einen zweiten Zustellversuch nach einem 4xx-Fehler versuchen. Bis jetzt waren alle Mail-Administratoren dankbar, auf diese Weise überhaupt vom nicht standardkonformen Verhalten ihres Systems zu erfahren. (un)

MARCEL LOHMANN

ist Softwareentwickler bei der Gesellschaft für Informatik und Datenverarbeitungstechnologie mbH in Hannover.

Literatur

[1] Evan Harris; Greylisting; projects.puremagic.com/greylisting/whitepaper.html

[2] *iX*-Listing-Service; ftp.ix.de/pub/ix/ix_listings/2008/11

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Assistenten bauen in Java: Die Wizard API

Zauberhafte Dialoge

Thomas Künneth



In Betriebssystemen und Anwendungen leiten den Benutzer oft Wizards oder Assistenten durch Folgen von Dialogen. Auch Swing-Entwicklern steht dafür eine Open-Source-Klassenbibliothek zur Verfügung.

Assistenten (Wizards) erfragen beim Benutzer in mehreren aufeinander folgenden Dialogschritten Informationen, um eine bestimmte Aktion ausführen zu können. Beispielsweise muss eine E-Mail-Anwendung vor dem Anlegen eines neuen Kontos seine Kennung und sein Passwort sowie die E-Mail-Adresse und den Servernamen ermitteln. Installations- oder Setup-Programme benötigen vor dem Kopieren den Pfad des Zielverzeichnisses sowie Installationsart beziehungsweise -umfang. Außerdem können Anwender oft festlegen, ob Symbole auf dem Desktop erscheinen sollen.

Wizards kommen auf allen aktuellen Plattformen vor. Zwar unterscheiden sich die einzelnen Implementierungen im Detail, doch bestimmte Merkmale praktisch immer vorhanden. Das wahrscheinlich wichtigste ist (auch wenn es auf den ersten Blick trivial wirkt) die Navigierbarkeit zwischen Dialogschritten mit „Zurück“ und „Weiter“, verbunden mit der Möglichkeit, den Assistenten vorzeitig abzubrechen. Damit dies klappt, sollte das Durchlaufen seiner Seiten keine unwiderruflichen Aktionen auslösen. Die eigentliche Arbeit findet in der Regel erst statt, wenn der Anwender auf „Fertig(stellen)“ klickt. Außerdem zeichnet Assistenten aus, dass ihre Seitenabfolge zum Zeitpunkt des Aufrufs nicht vollständig festgelegt sein muss. Sie kann abhängig von Benutzereingaben variieren. Beispielsweise muss ein Installationsprogramm nur eine Modul- oder Paketauswahl anzeigen, wenn der Anwender nicht die Standardinstallation gewählt hat. Ein solcher Dialogfluss lässt sich nur mit baumartigen Strukturen abbilden. Schließlich hilft oft eine Übersicht über absolvierte und gegebenenfalls noch folgende Schritte dem Benutzer, während der Arbeit mit dem Assistenten den Überblick zu behalten.

Auf wizard.dev.java.net steht Swing-Entwicklern eine Klassenbibliothek zur Verfügung, die das Erstellen und Anzeigen von Assistenten vereinfachen möchte. Das unter der Common Development and Distribution License veröffentlichte Projekt war ursprünglich als Ersatz für die Wizard API von Netbeans gedacht, was sich noch in den verwendeten Paketnamen zeigt. Die ab Java 1.4 lauffähige Bibliothek lässt sich aber in jeder Swing-Anwendung einsetzen. Damit man sie nutzen kann, muss sich die Datei *wizard.jar* im Klassenpfad befinden, die auf der Projekt-Homepage zum Herunterladen bereitsteht. Dort liegt auch die Javadoc-Dokumentation in Form des Archivs *WizardAPI.zip*. Die Quelltexte lassen sich gegebenenfalls aus dem zum Projekt gehörenden CVS-Repository auschecken.

Von einem Dialog zum nächsten

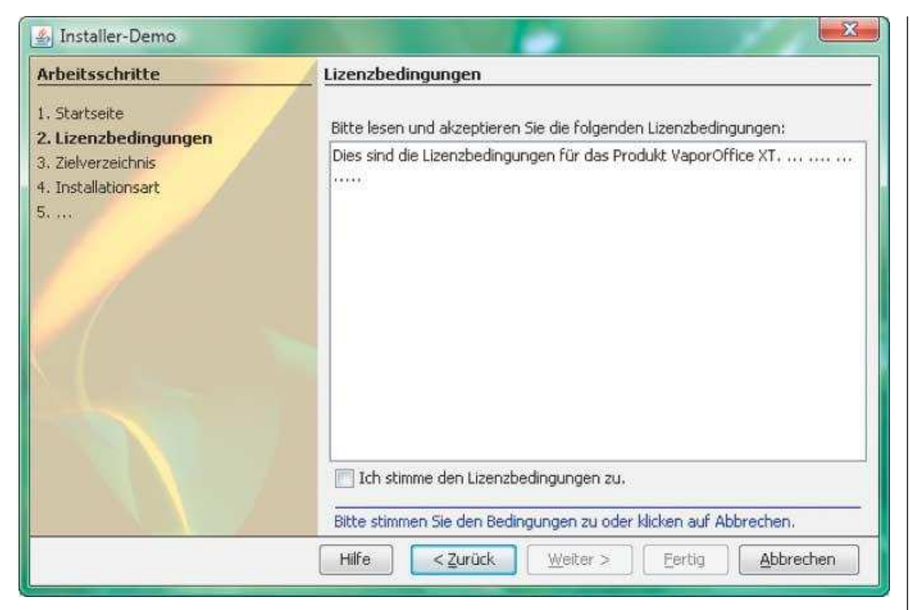
Assistenten definiert die Wizard API als eine Folge von Dialogschritten, die Einstellungen oder Eingaben des Benutzers entgegennehmen und als Schlüssel-Wert-Paare in einem Objekt des Typs *java.util.Map* speichern. Nachdem der Anwender „Fertig“ angeklickt hat, übergibt der Wizard diese Map an eine *finish()*-Methode. Sie erzeugt ein (im Prinzip beliebiges) Objekt, das die Einstellungen widerspiegelt, und führt die eigentliche Arbeit aus. Dies kann auf Wunsch in einem eigenständigen Thread, also im Hintergrund, geschehen. Neben fest vorgegebenen Panel-Abfolgen sind Verzweigungen vorgesehen, sodass ein Assistent dynamisch auf Benutzereingaben reagieren kann. Da sich Eingaben prüfen lassen, ist es beispielsweise möglich, Seitenwechsel zu unterbinden, bis der Anwender ein bestimmtes Feld ausgefüllt oder ein Element angewählt hat.

Dialogschritte können Entwickler auf zwei Arten bauen. Am einfachsten

Listing 1: Auszug aus *Zusammenfassung.java*

```
@Override
public WizardPanelNavResult allowBack(String stepName,
    Map settings,
    Wizard wizard) {
  settings.remove(InstallationsartPanel.RB_ALLES);
  settings.remove(InstallationsartPanel.RB_AUSWAHL);
  return WizardPanelNavResult.PROCEED;
}
```


© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Mit der Wizard API lassen sich einfache Assistenten wie dieser Installationshelfer erstellen.

ist es, von der Klasse *org.netbeans.spi.wizard.WizardPage* abzuleiten. Ein solches Panel vereinfacht das Übernehmen von Benutzereingaben in die angesprochene Map. Denn für Standardkomponenten wie *JCheckBox* oder *JTextField* genügt es, sie einer *WizardPage* hinzuzufügen und die Methode *setName()* der Komponente aufzurufen. Dies könnte folgendermaßen aussehen:

```
WizardPage seite =
  new WizardPage("schritt-1", "Der erste Schritt");
JTextField eingabe = new JTextField(20);
eingabe.setName("eingabe");
seite.add(eingabe);
```

Eingegebenen Text übernimmt der Wizard automatisch unter dem Schlüssel *eingabe* in die Map. Damit das klappt, muss der Aufruf von *setName()* erfolgen, bevor die Komponente der *WizardPage* hinzugefügt wird. Komponenten müssen übrigens keine unmittelbaren Kinder der *WizardPage* sein, sondern dürfen sich auch in verschachtelten Containern befinden.

Wizards erzeugen und anzeigen

Einen Assistenten, der aus dieser Seite besteht, erzeugt die folgende Anweisung:

```
Wizard wizard = WizardPage.createWizard(
   new WizardPage [] {seite});
```

WizardDisplayer.showWizard() zeigt den Assistenten an. Mit einem einfachen Cast liefert dieselbe Methode die vom Benutzer eingegebenen Werte:

```
Map ergebnis =
  (Map) WizardDisplayer.showWizard(wizard);
System.out.println(ergebnis);
```

WizardPage enthält zahlreiche Methoden. Das Verhalten des Dialogschritts lässt sich beeinflussen, indem man sie überschreibt. Beispielsweise ruft der Wizard für Benutzereingaben *validateContents()* auf. Dessen Rückgabewert steuert, ob der Assistent auf die Folgeseite wechseln darf oder ob er den Benutzer auf ein bestehendes Problem hinweist. Auch die Methoden *allowNext()* und *allowFinish()* beeinflussen mit ihren Rückgabeparametern die Navigierbarkeit innerhalb eines Assistenten.

InstallerDemo (siehe Abbildung oben) simuliert ein Installationsprogramm für die fiktive Bürosoftware Vapor Office XT. Seine vollständigen Quelltexte liegen auf dem *iX*-Listingserver (siehe *iX*-Link). Die Klassen *Zusammenfassung* und *Paketauswahl* der Anwendung zeigen das Überschreiben der angesprochenen Methoden. Das Beispiel in Listing 1 entfernt vor dem Zurückspringen auf die vorherige Seite des Assistenten zwei Elemente aus der Map, die die Benutzereingaben speichert. Weitere Klassen dieser Anwendung demonstrieren das zweite Vorgehen beim Erzeugen von Dialogschritten (siehe Listing 2): Die Klasse *StartseitePanelProvider* leitet von *org.net beans.spi.wizard.WizardPanel Provider* ab. Ihre Methode *createPanel()* ordnet

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Listing 2: Auszug aus *StartseitePanelProvider.java*

```
@Override
protected JComponent createPanel(WizardController
controller, String id,
        Map settings) {
  if (StartseitePanel.STEP_ID.equals(id)) {
    return new StartseitePanel();
  } else if (LizenzbedingungenPanel.STEP_ID.equals(id)) {
    return new LizenzbedingungenPanel(controller);
  } else if (ZielverzeichnisPanel.STEP_ID.equals(id)) {
    return new ZielverzeichnisPanel(controller);
  } else if (InstallationsartPanel.STEP_ID.equals(id)) {
    return new InstallationsartPanel(settings);
  }
  return null;
}
```

Listing 3: Auszug aus *InstallerDemoBranchController.java*

```
@Override
protected Wizard getWizardForStep(String step, Map settings) {
  if (InstallationsartPanel.STEP_ID.equals(step)) {
    if (Boolean.TRUE.equals(settings
          .get(InstallationsartPanel.RB_AUSWAHL))) {
      return ZWEIG_PAKETAUSWAHL;
    } else if (Boolean.FALSE.equals(settings
          .get(InstallationsartPanel.RB_AUSWAHL))) {
      return ZWEIG_ZUSAMMENFASSUNG;
    }
  }
  return null;
}
```

Listing 4: Auszug aus *InstallerDemoDeferredWizardResult.java*

```
@Override
public void start(Map settings, final ResultProgressHandle progress) {
  try {
    progress.setProgress("Dateien kopieren", 0, 3);
    warten();
    progress.setProgress("Leistung optimieren", 1, 3);
    warten();
    progress.setProgress("Installation abschließen", 2, 3);
    warten();
    progress.finished(getSummary(settings));
  } catch (Throwable thr) {
    progress.failed(thr.getMessage(), false);
  }
}
```

Listing 5: Auszug aus *InstallerDemoDeferredWizardResult.java*

```
private Summary getSummary(Map settings) {
  StringBuilder sb = new StringBuilder();
  sb.append("Die Installation ist abgeschlossen.\n");
  if (settings != null) {
    Set set = settings.keySet();
    Iterator iter = set.iterator();
    while (iter.hasNext()) {
      String key = (String) iter.next();
      sb.append(key + " = " + settings.get(key) + "\n");
    }
  }
  return Summary.create(sb.toString(), settings);
}
```

durch eine eindeutige Kennung identifizierbaren Dialogschritten eine Komponente zu, die den Schritt repräsentiert.

Welche Dialogschritte einem *WizardPanelProvider* zugeordnet sind, legt sein Konstruktor fest. Für *StartseitePanelProvider* sieht dies folgendermaßen aus:

```
public StartseitePanelProvider() {
  super("Installer-Demo", new String[] {
        StartseitePanel.STEP_ID,
        LizenzbedingungenPanel.STEP_ID,
        ZielverzeichnisPanel.STEP_ID,
        InstallationsartPanel.STEP_ID },
      new String[] {
        StartseitePanel.DESCRIPTION,
        LizenzbedingungenPanel.DESCRIPTION,
        ZielverzeichnisPanel.DESCRIPTION,
        InstallationsartPanel.DESCRIPTION });
}
```

Auch *WizardPanelProvider* definieren also vorgegebene Abfolgen von Dialogschritten. Bei einem Installationsprogramm ergibt sich aber unter Umständen die Notwendigkeit, Seiten zu überspringen. Beispielsweise sollte eine Paketauswahl nur erscheinen, wenn sich der Anwender für eine individuelle Auswahl der zu installierenden Funktionen entschieden hat.

Zwischen Ästen navigieren

Die Wizard API realisiert Verzweigungen mit der Klasse *org.netbeans.spi.wizard.WizardBranchController*. Ihre Methode *getWizardForStep()* entscheidet anhand der gerade angezeigten Seite sowie der bisherigen Benutzereingaben, welche Instanz der Klasse *org.netbeans.spi.wizard.Wizard* als Nächstes auszuführen ist. Verzweigungen basieren also darauf, Dialogschritte zu Teilassistenten zusammenzufassen und diese zu verschachteln.

In Listing 3 prüft der Code, ob der aktuelle Dialogschritt der Seite *Installationsart* entspricht. In diesem Fall wählt der Wizard auf Basis der Benutzereingaben den Teilassistenten *ZWEIG_PAKETAUSWAHL*. Er wurde auf die bekannte Weise erzeugt:

```
private static final Wizard
  ZWEIG_PAKETAUSWAHL = WizardPage
   .createWizard(new Class[] {
        Paketauswahl.class,
        Zusammenfassung.class },
      ERGEBNIS);
```

ERGEBNIS referenziert eine Instanz der Klasse *InstallerDemoResultProducer*. Sie implementiert das Interface *org.netbeans.spi.wizard.WizardPage.WizardResultProducer*. Ihre beiden Methoden *finish()* und *cancel()* aktiviert das Anklicken von „Fertig“ beziehungsweise „Abbrechen“. Innerhalb von *finish()* kann man aus den Werten der Map mit den Benutzereingaben ein Objekt erzeugen, das der Aufrufer des Assistenten als Rückgabeparameter erhält:

```
public Object finish(Map wizardData)
  throws WizardException {
    return new InstallerDemoDeferredWizard↵
                                    Result();
}
```

Eine besondere Form eines solchen Objekts bilden Instanzen der Klasse *DeferredWizardResult*. Sie ermöglichen das Ausführen länger laufender Tätigkeiten im Hintergrund. Solange sie andauern, zeigt der Assistent einen Fortschrittsbalken an (s. Listing 4). Die Hauptarbeit findet in der Methode *start()* statt.

Durch Aufrufen der Methode *setProgress()* erfährt der Anwender den Status der länger dauernden Tätigkeiten. Sind sie erfolgreich abgeschlossen, muss wie üblich ein Rückgabeobjekt erzeugt und an die Methode *finish()* übergeben werden.

Ist dieses übergebene Objekt eine Instanz des Typs *org.netbeans.spi.wizard.Summary*, stellt die Wizard API eine Seite dar, die das Ergebnis des Assistenten zusammenfasst (Listing 5). Die Klasse *Summary* stellt drei Factory-Methoden zum einfachen Erstellen von Zusammenfassungen zur Verfügung.

Fazit

Die Wizard API ist eine mächtige Klassenbibliothek, die das Erstellen selbst komplexer Assistenten stark vereinfacht. Die Einflussmöglichkeiten auf die Navigation sind umfassend. Länger andauernde Tätigkeiten, auch beim Wechsel zwischen Seiten, können Hintergrundprozesse übernehmen. Insgesamt ist die Nutzung der Bibliothek wärmstens zu empfehlen. (ck)

THOMAS KÜNNETH

arbeitet als Spezialist für Client-Technologien im Team Anwendungsarchitektur einer großen Bundesbehörde. Neben zahlreichen Artikeln hat er zwei Bücher über Java und Eclipse veröffentlicht.





© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Comics als Abbild des Alltagslebens

Täglicher Wahnsinn

Diane Sieger

Nicht nur Drogen machen süchtig. Für manche sind es Computerspiele, andere können nicht von Sudoku oder vom Comic-Lesen lassen. Letztere profitieren von den täglich wechselnden Veröffentlichungen im Web.

Viel hat sich in den letzten 15 Jahren im World Wide Web getan, seit das CERN die WWW-Technik in die Public Domain gegeben hat. Während es im Juni 1993 ganze 130 Webserver weltweit gab, hat heute jeder, der was auf sich hält, seine eigene Homepage. Da wundert es nicht, dass Google mittlerweile rund 29 400 Treffer für „Gerhard Seyfried“, liefert, den von Torsten Beyer vor neun Jahren in seinem Beitrag „Zapf, Ding, Bats …“ (www.heise.de/ix/artikel/1999/09/142) noch schmerzlich vermissten Autor von Anarcho-Comics.

Gleich an zweiter Stelle taucht Seyfrieds Hompage auf (www.seyfried-berlin.de). Neben Hinweisen auf eigene Neuveröffentlichungen gibt es hier zum Beispiel Comic-Kostproben unter dem Menüpunkt „Cannabis Cartoons“, und unter „zeichenblog“ (in der linken Spalte ganz oben) erfährt man unter anderem die Wahrheit über den aktuellen Zustand des Turms von Pisa (wegen laufender Neueinträge eventuell dort unter „ältere Einträge“ nachsehen).

Etwas anders steht es um Beyers zweiten vermissten Helden: „der Gelbe Wastl“ liefert zwar mittlerweile ebenfalls einige Google-Treffer, die führen aber vor allem zu Amazon oder auf den „Comic-Marktplatz“. Ein Online-Genuss der alten Geschichten ist nicht drin. Wer in Kindheitserinnerungen schwelgen will, muss schon ein paar Euro für ein antiquarisches Heftchen investieren.

Dennoch lohnt sich nach neun Jahren ein erneuter Blick auf das Internet-Comic-Geschehen. Nach wie vor populär ist die Netzkultfigur Dilbert, der Ingenieur, der in seinem Cubicle in einem Großraumbüro dem alltäglichen Wahnsinn ausgesetzt ist. In vielen Büros weltweit ist die erste Amtshandlung des Tages das Aufrufen von www.dilbert.com, um in den Genuss des täglich wechselnden Comicstrips zu kommen. Wer den morgendlichen Surfgang zur Dilbert-Website scheut, kann sich das Dilbert-Widget, widget.dilbert.com, installieren, und bekommt jeden Tag den neuesten Strip frisch auf eine Plattform seiner Wahl geliefert (Facebook, Myspace, Blogger etc.).

Der Kampf für Open Source

Ebenfalls um alltägliches Bürogeschehen dreht es sich bei www.userfriendly.org. Die Mannschaft des fiktiven Internetproviders „Columbia Internet“ kämpft in ihren Geschichten für Open-Source-Software und Linux und lässt immer wieder ihre negative Meinung zu Microsofts Produkten in ihre Dialoge einfließen. Die Userfriendly-Fangemeinde hat sogar ein eigenes Portal: Unter ufies.org können sich regelmäßige Leser untereinander austauschen und durch eine Reihe Links zu verwandten Themen klicken. Bis zum Jahr 2003 gab es übrigens auch eine deutsche Übersetzung der täglichen Comics, die noch heute unter www.comic-strips.de/benutzer/bf_heute.htm im Archiv einsehbar sind.

Einer der weltweit beliebtesten Comics – zumindest laut Wikipedia (en.wikipedia.org/wiki/Penny_Arcade_(webcomic)) – ist Penny Arcade. Der regelmäßig unter www.penny-arcade.com/comic/ erscheinende Strip widmet sich voll und ganz dem Thema Videospiel und kommt mitunter wenig jugendfrei daher. Im angeschlossenen Forum (forums.penny-arcade.com) können sich Fans von Comic oder Videospielen im Allgemeinen austauschen und Lob oder Kritik äußern. Und ist man erstmal süchtig nach der täglichen Dosis Penny Arcade, kann man sich im Merchandise Shop (www.pennyarcademerch.com) das passende Fan-Outfit bestellen.

Die Abkürzung PvP steht für Player versus Player und ist der Titel eines Comicstrips von Geeks für Geeks. Typische Geek-Themen wie Herr der Ringe, Star Trek, Apple Computer und Kaffee werden unter www.pvponline.com an fünf Tagen pro Woche in Szene gesetzt. Da sich der Einstieg für neue Leser, die mit den Protagonisten noch nicht vertraut sind, nicht ganz einfach gestaltet, gibt es eine Vorstellung der Hauptpersonen mit einer kleinen Übersicht über die wichtigsten Handlungsbögen aus der Vergangenheit (www.pvponline.com/new-readers/).

Etwas akademischer geht es bei PhD zu. Hierbei handelt es sich zwar um Geschichten rund um eine Gruppe Doktoranden, die Abkürzung steht jedoch vielmehr für „Piled higher and deeper“ und verdeutlicht das Chaos, mit dem die junge Truppe regelmäßig zu kämpfen hat. Wer sich den Comic-Strip von nun an täglich zu Gemüte führen möchte, sollte sich zunächst unter www.phdcomics.com/comics/aboutcomics.html umschauen und sich mit dem namenlosen Titelhelden der Geschichte sowie seinen Freunden Cecilia, Mike und Tajel vertraut machen. Unter derselben URL gibt es eine Auswahl der beliebtesten Strips für diejenigen, die nicht einer täglichen Leseroutine verfallen möchten. Nach dem Bekanntmachen mit den Protagonisten fällt es leicht, dem täglichen Wahnsinn entweder auf der Webseite (www.phdcomics.com/comics.php), im RSS Reader oder eingebunden auf der eigenen Homepage zu folgen.

Nicht ganz so intellektuell gibt sich www.starslip.com. Das ehemalige Kriegsraumschiff Slip Crisis ist zum Museumsschiff umgebaut worden, um unkultivierten Lebensformen ein kultiviertes Leben nahezubringen. Täglich liefert die Museums-Crew Geschichten, in denen es um Raumpiraten, Zeitreisen, böse oder auch niedliche Außerirdische und andere Verrücktheiten geht.

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Hier gibt es ebenfalls eine Abteilung für neue Leser (www.starslip.com/guide/), in der die Figuren und wichtige Handlungsstränge für ein besseres Verständnis erläutert werden. Und wer dem Autor mal beim Zeichnen der Starslip-Comics über die Schulter schauen möchte, sollte sich Kristofer Straubs Youtube-Video (www.youtube.com/watch?v=PPqqiFR26ZY) ansehen – dort gibt es einiges zu lernen.

Dem „Nochnichtsüchtigen", dem das tägliche Lesen eines Comics oder gar einer Fortsetzungsgeschichte zu viel ist, bietet sich das Verfolgen des vierzehntägig erscheinenden Ministrips „Die Dramatik der Dinge" von Katharina Greve an. Unter www.electrocomics.com/weekly/weeklydata/greve/html/de_greve1.html philosophieren Alltagsgegenstände wie Coladosen, Strohhalme oder Parkbänke über menschliche Themen. Ein Blick lohnt sich auch auf die englische Version, da manche Comics nur in einer der beiden Sprachen veröffentlicht zu sein scheinen.

Sollte das Interesse über das Lesen von Online-Comic-Strips hinausgehen, liefert Wikipedia unter de.wikipedia.org/wiki/Comic eine Ausgangsbasis für Hintergrundinformationen. Hier wird erklärt, welches der erste regelmäßig in einer Tageszeitung erscheinende Comic war, und was es mit dem Klischee, dass Comics nur für kindliche und jugendliche Männer gedacht sind, auf sich hat.

Nach all den witzigen und spannenden Comics hat vielleicht manch einer Lust bekommen, selbst einen Strip zu entwerfen. An Ideen wird es den meisten bestimmt nicht mangeln, denn der alltägliche Wahnsinn rund um Computer, Arbeit und Kollegen bietet genug Material für eine zeichnerische Umsetzung. Also auf zu pixton.com/home, nach kurzer Anmeldeprozedur stehen dort die nötigen Tools zur Verfügung, um mit dem Kreieren des ersten eigenen Werks zu beginnen. Und wer noch weiteres Handwerkszeug benötigt, um mit dem Comicschreiben loszulegen, kann sich zunächst den Step-by-Step Guide „Creating your own Internet Comic Strip" zu Gemüte führen. Unter www.somethingawful.com/d/guides/guide-creating-your.php wird genauestens erklärt, welche Elemente ein erfolgreicher Comic-Autor berücksichtigen sollte. (ka)

URLs auf einen Blick

www.heise.de/ix/artikel/1999/09/142/
www.seyfried-berlin.de
www.dilbert.com
widget.dilbert.com
www.userfriendly.org
ufies.org
www.comic-strips.de/benutzer/bf_heute.htm
en.wikipedia.org/wiki/Penny_Arcade_(webcomic)
www.penny-arcade.com/comic/
forums.penny-arcade.com
www.pennyarcademerch.com
www.pvponline.com
www.pvponline.com/new-readers/
www.phdcomics.com/comics/aboutcomics.html
www.phdcomics.com/comics.php
www.starslip.com
www.starslip.com/guide/
www.youtube.com/watch?v=PPqqiFR26ZY
www.electrocomics.com/weekly/weeklydata/greve/html/de_greve1.html
de.wikipedia.org/wiki/Comic
pixton.com/home
www.somethingawful.com/d/guides/guide-creating-your.php

Wer weitere URLs zum Thema kennt, hat die Möglichkeit, sie der Online-Version (www.heise.de/ix/artikel/2008/11/154/) hinzuzufügen.

Vor 10 Jahren: Vor 10 Jahren

Die November-Ausgabe 1998 von „*iX* – Magazin für professionelle Informationstechnik" war ein richtig dickes Heft, ein Geburtstagsschmöker.

Gefeiert wurde nichts weniger als 10 Jahre einer Zeitschrift, die 1988 als „*iX* – Multiuser Multitasking Magazin" gestartet worden war. Anfangs als Sonderheft der c't, ab 1999 als eigenständige Zeitschrift (was wir 2009 als 20-jähriges Jubiläum feiern, d. Red.), stand das Kürzel „*iX*" laut Eigenwerbung für „Unix und mehr". Das „mehr" waren dabei die PC-Netzwerke (Multiuser) und die internationalen Datennetze (Multikulti).

Vor 10 Jahren feierte man auch den Abschied vom Unix-Bezug. Professionelle Informationstechnik, das ist etwas ganz anderes als ein Betriebssystem in 256 Varianten mit 42 Oberflächen. Und dennoch kam die Jubiläumsnummer nicht von Unix los: zwölf eng bedruckte Seiten mit Stellenanzeigen (auch das ein denkwürdiger Rekord) kündeten davon, wie hoch der Bedarf an Unix-Fachkräften war: Es war praktisch keine Stelle ausgeschrieben, in der nicht Unix-Kenntnisse verlangt wurden. Selbst bei einem einsamen Inserat, in dem ein „Systemberater NT/Microsoft BackOffice" gesucht wurde, findet sich im Unterpunkt die Anforderung „Erfahrung in der Unix-Systeminstallation/-betreuung".

Werfen wir also zur Feier der Feier des Starts unseren virtuellen DeLorean an und verstellen noch einmal den Jahreshebel. Vor 20 Jahren schrieb der Autor dieser Zeitreisen über eine Ankündigung von IBM, dass Unix nunmehr die kritische Masse erreicht habe und man sich ab sofort im großen Stil an der Entwicklung beteiligen werde. Für die neu entstehende *iX* wurde daraus ein längerer Artikel über die 1988 gegründete Open Software Foundation. Ein einheitliches Unix sollte entstehen, solide und fest, wie es nur ein Industriestandard sein kann, an den sich dann alle halten müssen. Das beschlossen zumindest die Gründungsmitglieder Apollo, DEC, Bull, Hewlett-Packard, IBM, Nixdorf und Philips.

Nun besteht, nach einem geflügelten Wort von Friedrich Engels, die Probe des Puddings im Essen des Puddings. Flugs interviewte die neue Zeitschrift *iX* den frisch gebackenen OSF-Vorsitzenden David Tory. Das Ergebnis erschien nur in stark reduzierter Form: Die Pressestellen aller Gründungsmitglieder wollten erst ein Auge auf den Text werfen. Diese „Autorisierung", ein Unding im freien Journalismus, war zumindest im akademisch geprägten Unix-Umfeld unbekannt. Unix mochte zwar kein russischer Lastwagen sein, wie DEC-Chef Ken Olson damals witzelte, doch hinterließ das Verhalten der neuen OSF schon einen „russischen" Beigeschmack.

Immerhin, der Pudding, gerührt aus dem Einheitsversprechen, war angetestet. „Das haben wir noch nie gemacht", begann in *iX* 11/98 auch die „iXtory" von Chefredakteur Seeger mit einem Rückblick auf die ersten 10 Jahre, eine Klage der Hersteller zitierend. Denn bis dato hatte keine Zeitschrift teuerste IT-Systeme vor Ort getestet, wurden Ankündigungen der großen Player nur geschluckt. Seeger: „Wir wollten aber. Wir hatten uns in den Kopf gesetzt, über EDV nicht nur vom Hörensagen zu berichten, sondern alles ins Testlabor zu holen, was man auf einem Lastwagen transportieren konnte." Und die Lastwagen rollten an … *Detlef Borchers*

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

MEHR KBYTES

Webentwicklung

Um Websites zu erstellen, müssen Designer und Programmierer (vielleicht in Personalunion) Verschiedenes in Betracht ziehen, darunter Ästhetik, Webstandards, Benutzbarkeit und Web-2.0-Eigenschaften. Ohne Letztere hätte man den Auftrag wahrscheinlich nicht bekommen. Um mit den Standards zu beginnen: Websites, die ohne CSS auskommen (wollen), dürften mittlerweile gegen Null gehen. Ingo Chao und Corina Rudel haben bei Galileo „Fortgeschrittene CSS-Techniken“ veröffentlicht. Wer mehr als nur ein paar Selektoren und Deklarationen, sondern Sites insgesamt formatieren will, findet in diesem Buch eine gründliche Darstellung dessen, worauf bei CSS zu achten ist – inklusive abweichenden Browserverhaltens. Vertikale wie horizontale Elementanordnung, Floating, Inline-Formatierung sowie Positionierung und den z-Index behandeln Autor und Autorin detailliert; dasselbe gilt für Hintergrundbilder und Tabellen mit CSS. Wie man ein Layout prüft (Debugging), nimmt circa 60 Seiten ein. Ihnen folgen komplexere Layouts: Navigation, Mehrspaltigkeit. Gut geeignet für stringentes Durcharbeiten sowie Nachschlagen.

James Kalbach hat sich eines scheinbar geringen Teils des Webdesigns angenommen: der Navigation. In Fortsetzung eines Bandes von Jennifer Fleming aus dem Jahre 1998 behandelt er, warum dieser Aspekt so wichtig ist. Schließlich müssen Surfer schnell finden, was sie suchen, damit sie nicht aufgeben. Grundlagen, welche Elemente eine Navigation haben kann und wie man sie beschriftet, stehen am Anfang. Dem schließt sich ein circa 150 Seiten umfassendes Framework fürs Design an. Spezielles wie Tagging und das Entwerfen von Rich-Web-Anwendungen runden den informativen Band ab.

Javascript, eine der wichtigen Ingredienzen des Web 2.0, sei hier nicht unberücksichtigt. Cameron Adams und weitere Autoren haben für den australischen Sitepoint-Verlag „The Art & Science of Javascript“ zusammengestellt, das ein paar Leckerbissen für Programmierer beinhalten soll. Spaß mit Tabellen, heißt es im ersten Kapitel, des Weiteren geht es um das HTML5-Element *canvas*, Metaprogrammierung, ein 3D-Labyrinth sowie Mashups. Wer Ideen benötigt …

Dass Webdesign etwas mit Kunst zu tun haben könnte, unterstellt spätestens die Tatsache, dass der Taschen-Verlag Bücher zu diesem Thema ins Programm nimmt. Julius Wiedemann ist seit einiger Zeit für derlei im Verlag zuständig und hat – nach anderen Bänden – jetzt zusammen mit dem Erfinder des „Favourite Website Award“, Rob Ford, einen Band herausgegeben, der laut Untertitel Tipps und Tricks der Crème de la Crème der Werbeagenturen beinhaltet.

Von der Aufmachung her erinnert wenig an ein IT-Buch, mehr an einen Ausstellungskatalog, was so unzutreffend ja nicht ist. Wer Listings sucht, braucht andere Lektüre. Wer hingegen eine knappe Zusammenstellung von Ratschlägen mit vielen Beispielsites goutiert, sollte das mit einem Gummiband zusammengehaltene Werk studieren. In sechs Abschnitten, die von „Interface & Design“ über „Technology & Programming“ bis zu „E-Commerce“ reichen, geben wechselnde Agentur-Mitarbeiter ihre Dos & Don’ts zu Unterthemen preis. Das schönste Don’t stammt von Andy Foulds: „Schenken Sie guten Ratschlägen wie diesen nicht zu viel Beachtung“. Ein Blätterbuch, das immerhin ein Teilkapitel zu Webstandards bietet.

Projektmanagement und Enterprise, Kochen und Origami – alle haben anscheinend ein Update auf Version 2.0 erfahren. Angesichts der Flut an Versionssprüngen, die vereinzelt bis 3.0 reichen, mag man fast nicht mehr hinlesen. Zu Unrecht, wie das von Willms Buhse und Sören Stamer herausgegebene „Enterprise 2.0 – Die Kunst, loszulassen“ zeigt. Der bei Rhombos verlegte Band versammelt Beiträge, die von der Begriffsbestimmung über Erfahrungsberichte bis zum Tagebuch einer Chefsekretärin reichen.

Wenn Unternehmen die Kunst loszulassen lernen wollen, bedeutet das immer ein Weniger an Hierarchie. Wie es Sören Stamer in seinem Essay über die Erfahrungen bei Coremedia ausdrückt, ersetzt eine Feedback-Schleife die Kontrolle. Was das für Unternehmen bedeuten kann, beleuchten Beiträge, die etwa die interaktive Wertschöpfung anhand einer T-Shirt-Firma darstellen oder aus Firmensicht (SAP, Vodafone, Nokia) Erfahrungen mit dem neuen Web wiedergeben. Gut lesbar, selbst wenn das Management nicht gleich vor Begeisterung überschäumen sollte.

Nach gut drei Jahren Gewöhnung an den Begriff haben Vieweg + Teubner-Autoren einen wissenschaftlichen Blick auf das Phänomen Web 2.0 geworfen. Herausgegeben von Paul Alpar und Steffen Blaschke versammelt „Web 2.0 – Eine empirische Bestandsaufnahme“ Aufsätze zu Blogs, Wikis und sozialen Netzen sowie Nachrichten. Sie analysieren die Top 100 der deutschen Blogosphäre und Geschlechterunterschiede dort. Bei Wikis geht es nicht nur um Wikipedia, sondern außerdem um deren Bedeutung in Unternehmen. Selbst Second Life wird betrachtet. Keine Einführung, stattdessen wissenschaftliche Betrachtungen des Status quo. *Henning Behme*

Cameron Adams, James Edwards, Christian Heilmann, Michael Mahemoff, Ara Pehlivanian, Dan Webb, Simon Willison; **The Art & Science of Javascript**; Collingwood, Australien (Sitepoint) 2007; 258 Seiten; US-$ 39,95 (Paperback)

Paul Alpar, Steffen Blaschke (Hrsg.); **Web 2.0 – Eine empirische Bestandsaufnahme**; Wiesbaden (Vieweg + Teubner) 2008; 336 Seiten; € 49,90 (Paperback)

Willms Buhse, Sören Stamer (Hrsg.); **Enterprise 2.0 – Die Kunst, loszulassen**; Berlin (Rhombos) 2008; 267 Seiten; € 29,80 (Paperback)

Ingo Chao, Corina Rudel; **Fortgeschrittene CSS-Techniken**; Inkl. Debugging; Bonn (Galileo) 2008; 424 Seiten zzgl. DVD; € 39,90 (gebunden)

Rob Ford, Julius Wiedemann (Hrsg.); **Erfolg im Web: worauf es ankommt**; Tipps und Tricks der besten Werbeagenturen der Welt; Köln (Taschen) 2008; 334 Seiten; € 29,99 (Paperback)

James Kalbach; **Handbuch der Webnavigation**; Die User-Erfahrung optimieren; Köln (O’Reilly) 2008; übersetzt von Michael Gerth; 397 Seiten; € 49,90 (Paperback)

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Peter Buxmann, Heiner Diefenbach, Thomas Hess

Die Softwareindustrie

Ökonomische Prinzipien, Strategien, Perspektiven

Berlin, Heidelberg 2008
Springer-Verlag
216 Seiten
39,95 €
ISBN 978-3-540-71828-4

Wie wird aus Software Geld? Klar, indem man sie verkauft oder vermietet. Aber wie erklärt sich der Geschäftserfolg von Software-Riesen, wie macht ein Anbieter Umsatz, der seine Software verschenkt und was motiviert Open-Source-Entwickler? Die Antworten auf diese Fragen und viele weitere wissenswerte Informationen aus der Software-Ökonomie erhält der Leser in diesem Buch.

Die Entwicklung von Software kann teuer sein. Doch anders als bei materiellen Gütern verursacht die wachsende Zahl an Kopien nur minimale Kosten. Zudem existiert mit dem Internet ein globaler Vertriebskanal. Sind die Entwicklungskosten eingespielt, erzielt jede weitere verkaufte Kopie einer Software einen Deckungsbeitrag. An die Stelle der für materielle Güter oder Dienstleistungen üblichen Kosten-Plus-Kalkulation tritt daher eine Preisbildung, die sich am Wert der Software für den Kunden bemisst. Den maximalen Gewinn erzielt ein Unternehmen somit, wenn jeder Kunde den Preis bezahlt, der möglichst dem Wert entspricht, den die Software für ihn hat.

Da Software oft dem Austausch von Informationen und der Vernetzung dient, steigt ihr Wert mit der Zahl ihrer Nutzer. Wer Bürodokumente verschicken möchte, dürfte einem weit verbreiteten Format den Vorzug geben. Und wer erst einmal die Verwendung einer bestimmten Bürosoftware erlernt hat, verspürt wenig Veranlassung, auf ein anderes Produkt umzusteigen. Um hohe Nutzerzahlen und damit einen entsprechenden Netzeffekt zu erzielen, kann es daher sinnvoll sein, Software zu verschenken und den Umsatz durch Werbung oder Zusatzprodukte zu erzielen.

Bei der Open-Source-Entwicklung treten neben die kommerziellen Motive wie den Aufbau eines guten Rufes ideelle Ziele wie der Wunsch nach Informationsfreiheit und der Beschränkung der Marktmacht von Softwareriesen.

Die Autoren stellen die Softwareökonomie umfassend und gut verständlich dar. Außerdem berücksichtigen sie aktuelle Themen wie SOA, modellgetriebene Entwicklung und Softwareproduktlinien. Das Werk hat Pioniercharakter und ist Informatikstudenten ebenso wie Dozenten uneingeschränkt zu empfehlen – darüber hinaus auch Managern, Vertriebsbeauftragten und Entwicklern.

DR. ULRICH EISENECKER



Johann-Peter Hartmann, Björn Schotte (Hrsg.)

Enterprise PHP 5

Serviceorientierte und webbasierte Anwendungen für den Unternehmenseinsatz

München, Wien 2008
Carl Hanser
250 Seiten
39,90 €
ISBN 978-3-446-22563-3

Am Anfang fällt der Blick auf die Geschichte und die deutschsprachige Community: Mailingliste, erstes Buch, erste Konferenz, Gründung der User Groups. Nach diesem Rückblick führen die Autoren Rapid Prototyping und Schnelligkeit sowie Werkzeuge der agilen Softwareentwicklung als Argumente für den Einsatz von PHP an. Die Verwaltung des Software-Lebenszyklus, das Testen von Software und die kontinuierliche Integration reißen sie ebenfalls an.

Im zweiten Kapitel führt Udo von Eynern in die Welt des Web 2.0 ein. Es geht unter anderem um die Verlagerung der Programmlogik vom Server in den Client. Ajax, MVC und SOA heißen die Schlagworte. Im Kapitel „Web 2.0: Praxis“ verdeutlicht Andreas Uhsemann die Umsetzung der praktischen Anwendungsmöglichkeiten des Web 2.0 mit Javascript und Frameworks wie Prototype, Scriptaculous, Dojo und anderen.

Kapitel 4 gibt einen gelungenen Überblick über die Sicherheitsaspekte von Webanwendungen (XSS und CSRF). Das Kapitel schließt mit einem kurzen Leitfaden für die Entwicklung sicherer Ajax-Applikationen. Insbesondere diesen Abschnitt sollte der Leser nur als Überblick verstehen; er kann (und will) Christopher Kunz’ und Stefan Essers „PHP-Sicherheit“ nicht ersetzen.

Sebastian Schürmann behandelt das Testen von Software zunächst als effektiven Teil des Entwicklungszyklus, danach diskutiert er Qualitätskriterien. Es folgen Test-Workflows, beispielsweise exploratives Testen, Regressions- und Akzeptanztests. Im Anschluss gibt der Autor eine gelungene Einführung in die Erstellung und Durchführung automatisierter Akzeptanztests mit den Werkzeugen des Selenium-Projekts.

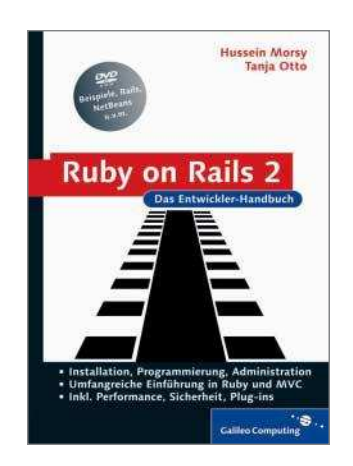
Jana Koch stellt den klassischen Ansatz für das Management eines IT-Projekts vor und legt den Schwerpunkt auf dessen Schwierigkeiten. Die agile Softwareentwicklung schickt sich unter anderem an, sie zu lösen. Nach einer einführenden Diskussion agiler Werte, Prinzipien und Methoden stellt Koch zunächst Extreme Programming (XP) und Crystal Clear vor. Ausführlicher behandelt sie im Anschluss den SCRUM-Prozess.

Thorsten Rinne zeigt die Grenzen der agilen Softwareentwicklung auf und beschreibt den Einsatz von PHP in Unternehmen, deren IT-Service-Management nach ITIL organisiert ist. Nach einer theoretischen Einführung wird der praktische Einsatz der ITIL-Richtlinien vorgestellt.

Die Autoren, keine Unbekannten in der PHP-Community, schöpfen aus ihrer Erfahrung in unternehmenskritischen Anwendungen. Der Leser profitiert davon und lernt unter anderem die Vorzüge von PHP in Bezug auf Rapid Prototyping und agile Entwicklung ebenso wie das Testen von Software kennen. Das Buch ist jedem zu empfehlen, der auf der Suche nach einem Leitfaden für die Entwicklung von PHP-Anwendungen im Unternehmensbereich ist.

SEBASTIAN BERGMANN

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Hussein Morsy, Tanja Otto

Ruby on Rails 2

Das Entwicklerhandbuch

Bonn 2008
Galileo Computing
700 Seiten
39,90 €
ISBN 978-3-89842-779-1

Ruby on Rails ist hip und kommt mehr und mehr in großen Webprojekten zum Einsatz. Hussein Morsy und Tanja Otto sind Rails-Enthusiasten der ersten Stunde. Ihr Entwickler-Buch, das sie Kompendium hätten nennen können, ist in vier Teile gegliedert. Im ersten, den Grundlagen, wird nach der Einführung und Installation der Software gleich eine erste Rails-Anwendung entwickelt. Hier zeigt sich schön, dass „Matz“ Matsumoto, der Erfinder von Ruby, eine Sprache geschaffen hat, die auch Nichtprogrammierer in Ansätzen leicht verstehen können. Im Kapitel zur Installation kommen Windows, Linux und Mac OS X vor, wenngleich die Autoren zu Recht anmerken, dass die Core-Entwickler von Rails ausschließlich auf Macs arbeiten. Eine Einführung zu objektorientierter Programmierung findet man hier nicht, Erfahrungen setzen die Autoren voraus, was sie aber erwähnen.

Der zweite Teil beherbergt zwei Kapitel mit Beispielapplikationen. Das erste der beiden führt mit einer Bookmark-Verwaltung in die Programmierung ein. Hier stellen die Autoren das Model-View-Controller-Konzept und dessen Umsetzung in Rails vor. Das Thema „Konventionen statt Konfigurationen“ zieht sich wie ein roter Faden durch Rails. Es gibt zahlreiche Standardeinstellungen, die das Programmieren mit Rails vereinfachen und dadurch kurzen, aussagekräftigen Code erzeugen. Themen wie Refactoring, Authentifizierung und Ausführungen zu Ajax runden dieses Kapitel ab. Des Weiteren geht es um Test-Driven Development anhand eines Fluggesellschaftsverwaltungssystems.

Rails als Framework begutachten Morsy und Otto ausführlich – auf gut 300 Seiten. Zunächst gehen die beiden in einem Kapitel auf das Erstellen von Rails-Projekten ein. Hier finden sich Dinge wie die Konsole, Debugging, Rake und Subversion. Den Abschluss bilden Kapitel zu Performancesteigerungen und Sicherheit (SQL Injection, Cross-Site Scripting, Session Hijacking et cetera). Das allerletzte Kapitel behandelt Deployment: fertige Rails-Applikationen auf einem Server zu veröffentlichen.

Morsys und Ottos Werk ist eine fundierte Einführung, die Nachschlagen durch einen ausführlichen Index unterstützt und dank der beigelegten DVD gleich mit Rails beginnen lässt.

KARSTEN KISSER

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.



Postfach 61 04 07, 30604 Hannover; Helstorfer Straße 7, 30625 Hannover

Redaktion
Telefon: 05 11/53 52-387, Fax: 05 11/53 52-361, E-Mail: post@ix.de
Abonnements: Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

Herausgeber: Christian Heise, Ansgar Heise

Redaktion: Chefredakteur: Jürgen Seeger (JS) -386

Stellv. Chefredakteur: Henning Behme (hb) -374

Ltd. Redakt.: Kersten Auel (ka) -367, Ralph Hülsenbusch (rh) -373, Bert Ungerer (un) -368

Jürgen Diercks (jd) -379, Christian Kirsch (ck) -590, Wolfgang Möhle (WM) -384, Susanne Nolte (sun) -689, André von Raison (avr) -377, Michael Riepe (mr) -787, Ute Roos (ur) -535

Redaktionsassistenz: Carmen Lehmann (cle) -387, Michael Mentzel (mm) -153

Korrespondent Köln/Düsseldorf/Ruhrgebiet:
Achim Born, Siebengebirgsallee 82, 50939 Köln,Telefon: 02 21/4 20 02 62,
E-Mail: ab@ix.de

Korrespondentin München:
Susanne Franke, Ansbacherstr. 2, 80796 München, Telefon: 089/28 80 74 80,
E-Mail: sf@ix.de

Ständige Mitarbeiter: Torsten Beyer, Detlef Borchers, Fred Hantelmann, Kai König, Michael Kuschke, Barbara Lange, Stefan Mintert, Holger Schwichtenberg, Susanne Schwonbeck, Christian Segor, Diane Sieger, Axel Urbanski, Axel Wilzopolski, Nikolai Zotow

DTP-Produktion: Enrico Eisert, Wiebke Preuß, Matthias Timm, Hinstorff Verlag, Rostock

Korrektorat/Chefin vom Dienst: Anja Fischer

Fotografie: Martin Klauss Fotografie, Despetal/Barfelde

Titelidee: ***iX;*** Titel- und Aufmachergestaltung: Dietmar Jokisch

Verlag und Anzeigenverwaltung:
Heise Zeitschriften Verlag GmbH & Co. KG, Postfach 61 04 07, 30604 Hannover;
Helstorfer Straße 7, 30625 Hannover; Telefon: 05 11/53 52-0, Fax: 05 11/53 52-129

Geschäftsführer: Ansgar Heise, Steven P. Steinkraus, Dr. Alfons Schräder

Mitglied der Geschäftsleitung: Beate Gerold

Verlagsleiter: Dr. Alfons Schräder

Anzeigenleitung: Michael Hanke -167, E-Mail: michael.hanke@heise.de

Assistenz: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigendisposition: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigenverkauf: PLZ-Gebiete 0–3, Ausland:
Oliver Kühn -395, E-Mail: oliver.kuehn@heise.de,
PLZ-Gebiete 8–9: Ralf Räuber -218, E-Mail: ralf.raeuber@heise.de
Sonderprojekte: Isabelle Paeseler -205, E-Mail: isabelle.paeseler@heise.de

Anzeigen-Inlandsvertretung: PLZ-Gebiete 4–7:
Karl-Heinz Kremer GmbH, Sonnenstraße 2, D-66957 Hilst,
Telefon: 063 35/92 17-0, Fax: 063 35/92 17-22, E-Mail: karlheinz.kremer@heise.de

Anzeigen-Auslandsvertretung:
Großbritannien, Irland: Oliver Smith & Partners Ltd. Colin Smith, 18 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX, UK, Telefon: (00 44) 20/79 78-14 40, Fax: (00 44) 20/79 78-15 50, E-Mail: colin@osp-uk.com

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 20 vom 1. Januar 2008.

Leiter Vertrieb und Marketing: Mark A. Cano (-299)

Werbeleitung: Julia Conrades (-156)

Teamleitung Herstellung: Bianca Nagel (-456)

Druck: Dierichs Druck + Media GmbH & Co. KG, Kassel

Sonderdruck-Service: Bianca Nagel (-456, Fax: -360)

Verantwortlich: Textteil: Jürgen Seeger; Anzeigenteil: Michael Hanke

***iX* erscheint monatlich**

Einzelpreis € 5,50, Österreich € 6,20, Schweiz CHF 10,70, Benelux € 6,70, Italien € 6,70

Das Abonnement für 12 Ausgaben kostet: Inland € 56,–, Ausland (außer Schweiz) € 63,–; Studentenabonnement: Inland € 42,–, Ausland (außer Schweiz) € 47,– nur gegen Vorlage der Studienbescheinigung (inkl. Versandkosten Inland € 8,30, Ausland € 13,30), Luftpost auf Anfrage.

iX-Abo+ (inkl. jährlicher Archiv-CD-ROM) jeweils zzgl. € 8,–

Für GI-, VDI-KfIT-, GUUG-, IUG-, LUG-, AUGE- und Mac-e.V.-Mitglieder gilt der Preis des Studentenabonnements (gegen Mitgliedsausweis).

Kundenkonto in Österreich:
Dresdner Bank AG, BLZ 19675, Kto.-Nr. 2001-226-00 EUR, SWIFT: DRES AT WX

Kundenkonto in der Schweiz: UBS AG, Zürich, Kto.-Nr. 206 P0-465.060.0

Abo-Service:
Heise Zeitschriften Verlag, Kundenservice, Postfach 810520, 70522 Stuttgart,
Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

Für Abonnenten in der Schweiz Bestellung über:
Thali AG, Aboservice, Industriestr. 14, CH-6285 Hitzkirch,
Telefon: 041/919 66 11, Fax: 041/919 66 77, E-Mail: abo@thali.ch, Internet: www.thali.ch (Jahresabonnement: CHF 111,–; Studentenabonnement: CHF 83,25)

Das Abonnement ohne Archiv-CD-ROM ist jederzeit mit Wirkung zur jeweils übernächsten Ausgabe kündbar. Das *iX-Abo*+ (incl. jährlicher Archiv-CD-ROM) gilt zunächst für ein Jahr und ist danach zur jeweils übernächsten Ausgabe kündbar.

Vertrieb Einzelverkauf (auch für Österreich, Luxemburg und Schweiz): MZV Moderner Zeitschriften Vertrieb GmbH & Co. KG, Breslauer Str. 5, 85386 Eching, Telefon: 089/319 06-0, Fax: 089/319 06-113, E-Mail: mzv@mzv.de, Internet: www.mzv.de

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Die gewerbliche Nutzung abgedruckter Programme ist nur mit schriftlicher Genehmigung des Herausgebers zulässig.

Honorierte Arbeiten gehen in das Verfügungsrecht des Verlages über, Nachdruck nur mit Genehmigung des Verlages. Mit Übergabe der Manuskripte und Bilder an die Redaktion erteilt der Verfasser dem Verlag das Exklusivrecht zur Veröffentlichung. Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Sämtliche Veröffentlichungen in ***iX*** erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.

Printed in Germany

© Copyright 2008 by Heise Zeitschriften Verlag GmbH & Co. KG

ISSN 0935-9680





Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

Anzeige

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.

November 2008



Auditing mit Oracle

Unternehmen müssen nicht nur die von ihnen verarbeiteten Daten vor dem Verschwinden und Verändern schützen. Wenn solche Vorfälle auftreten, müssen sie auch die Verantwortlichen identifizieren können. Dabei soll unter anderem das Auditing helfen, mit dem sich schädliche Handlungen protokollieren lassen.

Biometrische Zugriffs- und Zugangskontrolle

So sehr der Einsatz biometrischer Erkennungsmethoden für die innere Sicherheit kritisiert wird, so unumstritten ist ihr Nutzen bei einem zahlenmäßig begrenzten Nutzerkreis, etwa in Unternehmen. Doch nicht alle Verfahren sind für alle Einsatzbereiche tauglich. Was es alles gibt und was man wo am besten einsetzt, zeigt eine Marktübersicht.

Heft 12/2008 erscheint am 20. November 2008

Gerätekommunikation via Jabber und XML

Die zuverlässige und schnelle Nachrichtenübertragung zwischen verschiedenen Geräten ist eine immer wichtiger werdende Aufgabe im Bereich Embedded Systems. Dazu muss nichts neu erfunden werden: Das Instant-Message-System Jabber und XML können's richten.

IT-Equipment als Warmwasserquelle

Dass Server und anderes IT-Equipment die aufgenommene Energie zu fast 100 % als Wärme wieder abgeben, wissen vor allem diejenigen, die mit deren Entsorgung zu tun haben. Doch statt die Wärme einfach in die Umgebung abzulassen wie früher andere Industriezweige ihre Schadstoffe, nutzen erste Rechenzentren diese „sekundäre“ Energiequelle zum Heizen und zur Warmwasseraufbereitung.



CAD-Workstations gegen Gamer-PC

Grafische Arbeitsplätze im Konstruktions- und Simulationsbereich müssen andere Anforderungen erfüllen als die sonst üblichen Desktop-Rechner. Ähnliches gilt für Computer, die für Spiele aus der oberen e-Sport-Liga ausgelegt sind. Neben der Prozessorleistung und dem Speicherdurchsatz geht es vor allem um Grafikleistung. Die sollte eigentlich bei Workstations und Gamer-PCs auf ähnlichem hohen Niveau liegen.

Kein wichtiges Thema mehr versäumen!
Die aktuelle iX-Inhaltsübersicht per E-Mail
Man verpasst ja sonst schon genug!
www.heise.de/bin/newsletter/listinfo/ix-inhalt

Das bringen





DSL-Angebote ohne Telekom-Telefonanschluss

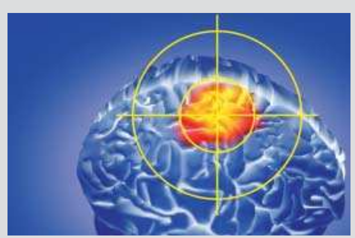
Centrino-2-Notebooks: Intels neue Plattform

RAID-Praxis unter Windows und Linux

Nettops: Schlanke Desktop-Rechnerlein

Heft 22/08 jetzt am Kiosk





Die Gedankenjäger: Mit welchen Methoden Wissenschaftler unser Denken und Fühlen entschlüsseln.

Wahlkampf im Web: Barack Obama bedient das soziale Netz so virtuos wie kaum ein anderer.

Heft 11/08 jetzt am Kiosk

TELEPOLIS

MAGAZIN DER NETZKULTUR



Stefan Höltgen: Geisterprozesse und Killerapplikationen – Der Computer im Film

Jörg Auf dem Hövel: Alte Pflanzen, neue Heilung? – Interview mit dem Experten für historische Pharmakologie Werner Dressendörfer

www.heise.de/tp/

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG. Veröffentlichung und Vervielfältigung nur mit Genehmigung des Heise Zeitschriften Verlags.